**Hoofdstuk 1 : ospf**

* Ospfv2 => ipv4
* Spf is beter dan rip want spf kan werken in grotere netwerken
* A link is a interface in the router , also a segement or a stub network
* State of a link => linkstate

Components of ospf

* Routing protocol message , hello messages, linkstate request …
* Database structure => ospf database , adjencensie table
* Algorithm => choose best route

Linkstate operation ;

* Establish neighbor adjencie : hello packet => zoekt neighbors als er is => establish neighbor adjencie
* Exchange linkstate advertisement
* Topology table
* Spf algorithm
* Choose best path

Single area ospf : alle routers in one area => area 0

Multi area ospf ; multiple areas , must be connecte to the backbone area 0, ABRS

Multi area ospf:

* Topology change in a area new spf algoritim to update the routing table. It takes time depending on the size of the area

Lsdb is te groot oplossing:

* Smaller routing table
* Reduced link state update overhead
* Redueced frequency of spf calculations

Ospfv3

* Ipv6 addressen
* Doet het zelfde als ospfv2

Ospf packets :

* Hello packets
* Database description packet
* Link state request packet
* Linkstate update packet
* Linkstate acknowledgement packet

Linkstate update packet

* Lsu word gebruikt wnr er lsr word gestuurd , ze worden ook gebruikt wnr de ospf routing updare wilt sturen
* Een lsu contain one or more lsa’s
* Lsu contains routing info for the destination

Hello packets

* Discover neighbors
* Elects dr,bdr alleen op multiacces networks
* Point to point networks dont need dr en bdr

Ospf states:

* Down state => no hello, router sends hello,
* Init state => hello received from neighbor, router id of the sending neighbor
* Two-wat state => biderctional,elect dr, bdr,
* Exstart state => point to point decide who send the dbd(hoogste router id)
* Exchange state => echange dbd,full state
* Loading state => ls ren lsu voor extra of nieuwe info,spf algrothim
* Full state => fully synchronized

Establish neighbor adjencie:

* Send to all router ospf router interfaces to see if there are neighbors : 224.0.0.5
* Router id 32bit
* Als de ospf router de hello packet krijgt en ziet dat die router id niet in de neighbor lijst zit dat maakt de router een establish neighbor adjencie with the other router

Exhange dbd’s

* Router 1 sends dbd to r2
* R2 acknowleges the dbd using lsACK packet
* R2 sends dbd to r1
* R1 acknowledges r2

Lsu are only send when a change is perceived and every 30 minutes it wil send a lsu automatically

Why is there a need for dr:

* Zonder dr wanneer je flooding lsa doet dan krijg je :
  + Creation of multiple adjencie
  + Extensive flooding of lsa’s
* Flooding lsa : lsa word gestuurd naar alle routers en triggers dat alle router ook lsa’s hierdoor gaat trafiek chaotisch worden
* Lsa’s dr : Als je een dr hebt en bv router 1 is een dr en router 2 wilt een lsa sturen dan gaat de lsa naar de dr en de dr stuur de lsa naar iedereen.op dit mannier stuurt niet elke router een lsa maar alleen de dr

Hoofstuk 2 : network security concepts

Current state of cyber security :

* Assets : value
* Vulnerability : weakness
* Threat : potential danger
* Exploit : take advantage of vulnerability
* Mitigation : counter-measure
* Risk : negativily affecting the organnistion . probabililty of occurrence of a event and its consequences

Vectors of network attacks :

* Attack vector => path to gain access to a server host or network
* Vector => insider or outside
* Dos => cant no more support legitimate users

An internal user such as employees can accidently or intentionly

* Steal and copy confidentaily data
* Compromise internal servers
* Disconnect a network
* Connect a infected usb
* Internal threats zijn gevaarlijker dan external

Data loss :

* Data is de belangrijkste asset
* Gevolgen :
  + Brand dammage
  + Loss of commpetitive advantage
  + Klanten kwijt
  + Loss of revenu
  + Fines and civil penalties
  + Cost
* Hoe kan dit gebeuren :
  + Email social networking
  + Unencrypted devices
  + Cloud storage
  + Removable media
  + Hard copy
  + Improper acces control
* Dlp

Threat actors:

* White hat hacker : legal purpose
* Grey hat hackers : commit crimes but not for personal gain or to cause damage
* Black hat hackers : crimes for personal gain or malicious reasons
* Threat actor => hacker

Evolution of hacking:

* Scritp kiddies
* Vulnerabilitie broker
* Hackitivist
* Cyber criminals
* State-sponsored

Cyber criminals

* Steal billions of dollars of businesses , operate in underground economy,targets are small businesses and consumers as well as large businesses

Hactivist :

* Not well organized
* Use fairly basic and free tools

State sponsored :

* Advanced code n undiscoverd software vulnerabilities

Threat actor tools

* Password crackers => repeadetly make guesses
* Wireless hacking tools => security vulnerabilities
* Network scanning and hacking tools => probe network devices
* Packter crafting tool => robe and test firewalls
* Packet sniffer => capture and anylize packets
* Rootkit detectors => file integrity checker
* Fuzzers to search => discover computer security vulenerbilities
* Forensic tools => SNIF ANY TRACE OF EVIdence of a existing computer
* Debugger : write exploit
* Hacking os => os with hacking tools
* Vulnerability exploits tools
* Vulenbility scanner

Many tools ar unix or linux based

Attack types :

* Eavesdropping attack => listen to network
* Data modification => alter data
* Ip address snooping attack => construnt a ip packet
* Password based attack =
* Denial of service
* Man in the middle
* Compromised key attack
* Sniffer attack

Malware

Virus

* Human action to progate and infect other computers
* Viruses can :
  + Delete files
  + Booting issues
  + Send sensitive data
  + Access email accounts
* Boot sector virus
* Firmware virus
* Macro virus
* Program virus
* Script virus

Trojan horse

* Program that looks useful but has malicious code => free online programs
* Types of trojan horses :
  + Remote access
  + Data sending
  + Desctructive
  + Proxy
  + ftp
  + security
  + dos
  + keylogger

Viruses and Trojan horses are only two types of malware that threat actors use. There are many other types of malware that have been designed for specific purposes.

other types of malware :

* adware
* ransomware
* rootkit => admin leve access to a computer
* spyware => get info and send to threat actor
* worm => to slow or disrupt network operations

common network attacks:

raconnaisance attack :

* means gather info
* access or dos attacks
* techniques for reconnaissance attack :
  + info querie on target
  + intiate ping sweep
  + intiat port scan of active ipaddress
  + run vulnerability scanners
  + run exploitation tools

access attack :

* passoword attacks
* spoofing attack : attempts to pose as a other devide by falsifying data
* trust exploitations : use unauthorized privileges to gain access to the system
* port redirections :use compromised system as a base to attack other targets
* man in the middle
* buffer overflow attack: exploits the buffer memory and overwhelm it with unexpected values

social engineering attack :

* manipulate individuals
* in person or telephone or internet
* prey on people’s weakness
* telephone scammers

social engenieering techiniek

* pretexting
* phising
* spear phising
* spam
* baiting
* impersonation
* tailgating
* shoulder surfing
* dumpster diving

**he Social Engineering Toolkit (SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks**

**dos end dos attacks**

* overwhelming quantity of traffiq
* maliciously formatted packets
* ddos almost the same as dos but the attacks originates from multiple coordinated sources=> zombie that can communicate with the cnc , the treat actor uses the cnc so that the zombies carry the ddos attack.

Ip vulnerabilities and threats

Ipv4 en 6

* IP does not validate whether the source IP address contained in a packet actually came from that source. For this reason, threat actors can send packets using a spoofed source IP address.
* Icmp attack => discover subnets and hosts to generate dos
* Ampliciatiion and reflection attacks : prevent legimate use to access services => dos
* Address spoofing attacks
* Man in the middle
* Session hijacking

Icmp attack :

* Gather info
* Counter measure is icmp acls
* Icmp messages that interest the threat actor:
  + Cmp echo request en reply
  + Icmp unreachable
  + Icm mask reply
  + Icmp redirects
  + Icmp router discovery

Amplification and reflection

* Create dos attacks
* Dns amplification and reflection en ntp amplification and reflection

Address spoofing attacks :

* False source ip addres , to pose as a legimate user
* Non-blind spoofing : inspect the reply packet from the target , can see the traffic being sent between host and target
* Blind spoofing : cannot see the traffic that is being sent between host and target => use dos attacks

Tcp and udp vulnerability

* Tcp services
  + Reliable deliviery : guarantee delivery
  + Flow control : multiple segment can be acknowledged with a single acknowledgement segment
  + Staefull communinication
  + Three way hand shake: if both side aggree to tcp connection only then data can be sent
* Tcp attacks
  + Tcp syn flood attack : exploit the three way handshake: so the threat actor send multiple syn request to a webserver the webserver sends multiple syn acks and wait but then the legimate user send a syn reques and now is the webserver confused en hierdoor kan de legimate user niet naar de webserver gaan
  + Tcp reset attack : terminate tcp communications
  + Tcp session hijacking : a threat actor takes over an already-authenticated host as it communicates with the target.

Udp segment header and operations

* No retransmisioon because not connection oriented , je krijgt geen replys
* Udp attack : uDP is not protected by any encryption. he lack of encryption means that anyone can see the traffic.
* Udp flood attack : gewoon vorm van dos

Ip services :

* Arp vulnerbilities :
  + Unsolicited arp reply (gratuitous arp)
  + First boot => inforl new mac address
  + Arp => doel is mack wetel van device
  + Arp cashe poisoning : doel target a victim host, and have it change its default gateway to the threat actor’s device. This positions the threat actor in between the victim and all other systems outside of the local subnet.
  + Passive arp poisoning => steal data
  + Active arp poisoning => modify data

Dns attacks :

* Dns resolver attack :
  + Dns cashe poisoning : spoofed records info to dns resolver to redirecto user to malicious sites
  + Sns amplification and reflection : use dos attacks
  + Dns resource utilization attack : consumes the resources of the dns opensolver
* Dns stealth attack : hide identity
  + Fast flux
  + Double ip flux
  + Domain generatio algorithm :
  + Dns shadowing attacks
* Dns tunnelling
  + It’s a method od sending data covertly by hiding it within the dns protocol
  + Opendns blocks dns tunnelling

Dhcp

Dhcp attacks

* Dhcp spoofing attack

Network security best pactrices:

* Confidentialy
* Integrity
* Availability

The defense in depth approach

* Secure communication across both public and private networks
* Vpn
* Ips
* Esa/was
* Aaa server

Firewalls

* Access control policy between networks
* All firewalls share common properties
  + Resisitant to networks attacks
  + All traffic flows through the firewall
  + Enforce the access control policy
* Benefits of firewall
  + Prevent the exposure of sensitive hosts, resource and applications to trusted users
* Limitations
  + Misconfigured firewall can have serious consequences=> single point of failure
  + Can slow down
  + Unauthorized traffic can be tunneled or hidden
* Ids e nips detect pattern in network traffic usiding signatutes, => to detect malicious activity
* Signature patterns Single packet en multi packet

Content security appliance :

* Esa : check emails
* Was : controlling web traffic

Cryptography :

* Four element of secure information
  + Data integrity
  + Origin authentication
  + Data confidentiality
  + Data non-repudiation
* Hash function
  + Md5 128 bit , niet aangeraden gebruike sha2 of 3
  + Sha hashing algoritm 160bit
  + Sha-2
  + Sha-3
  + Man in the middle kan de hash veranderen
* Hashing algorithms only protect against accidental changes and does not protect the data from changes deliberately made by a threat actor.
* Origin aurhincation : hmac
* Data confidentiality
  + Symmetric encryption : des , 3des , aes and uses one key
    - Block cypher and stream ciphers
  + Asymmetric : public and private key, rsa, difie helmann dss, dh

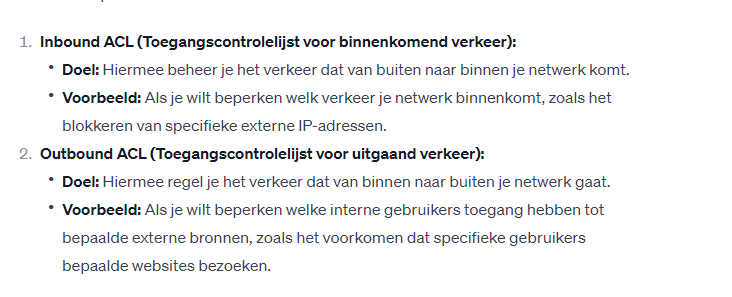
Hoofdstuk : acl concepts

What is a acl

* Filtering traffic
* Filter packets based on information
* By default a router does not have a acl configured
* Permit and deny statements > aces
* Waarvoor gebruik acl
  + Limit network traffic > increase performance
  + Traffic flow control
  + Basic leve of security
  + Provide priority of certain classes of network traffic

Packet filtering

* Packet filtering works at transport and network layer
* Standard acls use only source ip addres 1-99
* Extended acls use source destination addres and protocol 100-199 2000-2699
* Inbound acl => filter packets before they are routed out the outbound acl,
* outbound acl => filter packets after being routed out



* stappen die een inbound stand ipv4 acl doet : In het kort er word gekeken naar het pakket of het match met de ace rules van acl en als het match dat word er gekeken of het word permitted of denied. Als het niet match dan word het direct discarded.
* The last ace statement of an acl is always an implicit deny

Wildcard mask in acl:

* 32bit wildcard mask
* Zelfde als bij een ospf
* A specific ip addres => 0.0.0.0
* 0.0.0.255 is gewoon de /24 dat is een netwerk als je die als wildcard neemt
* Host => 0.0.0.0
* Any => accepts any address

Guidelines for acl creation

Limited number of acl per interface

* Duals stack => 4 acl’s

Guidelines for named acl

* Name => purpose of the acl
* Can contain alphanumeric characters
* Cannot contain spaces or punctuation
* Capital lettes

Acl

* Extended moet zo dicht bij de source of the trafic liggen
* Standerd acl zij dicht bij de destination , want als je een deny doet bij standard dan gaan alle pakketen gedropped ook al moet een pakket niet die richting uit

Factors infleuncing acl placement

* The extent of organisation control
* Bandwidth of the networks involved
* Ease of configuration

Hoofdstuk : nat for ipv4

Ipv4 privat addres space

* Nat translate private ip addressen to public ip acddressen
* With public ip address you can go to the internet

What is nat

* Primary use is to conserver public ipv4 addresses
* Translate ipv4 private addresses to public only when needed
* Privacy and security to a network
* Nat pool word gebruik wnr je een private naar public addres gaat
* Stub network is wanneer a een of meer netwerken met een single conection to neighboring network , on way in one way out
* Nat router operates at the border of a stub network
* Inside local => uw private addres
* Inside global => is uw public addres
* Outside local => destination
* Outside global => destination

Nat termonlogy

* Inside addres => device that is translate with nat
* Outside addres => destination
* Local address : address of inside the network
* global address : outside the network

static nat

* one to one mapping
* remain constaint
* useful for webserver , authorized personel via ssh

dynamic nat:

* Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis

Pat : port address translation

* Also known as nat overload
* Maps multiple privat ipaddressen to a single public ipaddress or a few addresses
* Tracked by port number
* Pat ensures that devices use a different port number for each session with a server on the internet

Next available port

* De source poort is de poort die met uw private meekomt en wanneer je pat gebruikt dan gebruikt die uw source poort en voegt die aan een public ip address op die manieer weet het waar de poort vandaan komt.
* Als de source poort al gebruikt word in pat dan word volgen available port gebruikt

Advantage nat

* Pat
* Increases flexibilty of connection to the public network
* Provides consistency for internal network addressing sheme
* Using rfc 1918 ipv4 addresse , nat hiedes the ipv4adresses of users and other devises som people consider this security but nat doesn’t apply security

Disadvantage of nat

* Voip is real time en gaat niet goed mee met nat want nat increases forwarding delays
* Nat delays zorgt voor dat isps become depleted, carier grade nat cgn
* End to end addressing is lost
* End to end ipv4 tracebility is lost
* Nat complicates the use of tunnelling protocols

Nat 64

* Ipv6
* Bij ipv6 is address space no issue
* Nat is unnecessary
* Ipv6 include its own private address space , unique local address ula
* Ula are meant for local communication within a site
* Tunnelling ipv6 is the processe of encapsulating ipv6 packet inside a ipv4 packet so that the packet to be transmittes over ipv4 only network
* NAT for IPv6 should not be used as a long-term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6

Hoofdstuk wan concepts:

Lans en wans

* Wide area network
* Wan operates beyon the geogrhapic scope of a lan

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Private and public wans

* Wan build in different types of organizations
  + An organization Connect users In different location
  + An isp Connect customers to the internet
  + Telecomuunicaiton that want to interoconnect isp’s
* Privat wan connection that is dedicated to single customer
  + Guaranteed service level
  + Consistent bandwidth
  + Security
* Public wan provided bij isp or telecomunincations
  + Leven bandwidth may vary
  + Do not gurante security

Wan topology

Point to point topology

Afbeelding met schermopname, lijn

Automatisch gegenereerde beschrijving

* Dedicated leased line connection from the corporate edge point to the provider networks
* Layer 2 transport services
* Packet from one site to another site
* Many point to point it becomes expensive

Hub and spoke topology

Afbeelding met lijn, diagram, schermopname, cirkel

Automatisch gegenereerde beschrijving

* Enables single interface on the hub router to be shared by all the spoke circuits
* Is a single homed topology , there is only one hub router and all communication must com through it
* Nadeel single point of failure

Dual homed topology

Afbeelding met lijn, cirkel, diagram

Automatisch gegenereerde beschrijving

* Enhanced network redundancy, loadbalancing,
* Disadvantage is that it is more expensive than a single homed en moeilijk om te implementen

Fully meshed topology

Afbeelding met cirkel, lijn

Automatisch gegenereerde beschrijving

* Site is een locatie in een wan
* Connect all sites
* The most fault tolerence topology

Partialy meshed topology

Afbeelding met cirkel, lijn

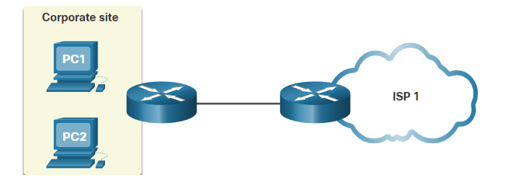
Automatisch gegenereerde beschrijving

* Connects many but not all sites

Carrier connection

* How a organistion connects to the internet
  + Signs a sla
  + Sla outlines services relating to the reliabilty and availability of the connection
* The service provider may or may not be the carier
* A carier owns and maintains the phusical connection and equipment between the provider and the customer
* Single carier wan connection or duals carier wan connection

Single carrier wan connection



* Organisation connects to only one service provider
* Disadvantage single point of failure

Duals carieer wan connection



* Provides redundancy and increases network availability
* Separate sla with two different service providers
* Different cariers
* More expensive

Evolving network

Small network

* 15 employees small office
* Single lan connected to a wireless router for sharinf data
* Connection to the internet is with a common broadband => dsl

Campus office

* Several floors of a building
* Campus area network
* CAN interconnect several lan within a limited geogrhapical area
* Muitiple lans
* Multiple switches
* Dedicated servers for email,data transfer, file storage, firewall, inhouse it staff

Branch networ:

* Regional sites in other cities? Meerder building connected to each other
* Metropolitan area network
* To connect to the central office, branch offices in nearby cities used private dedicated lines through their local service provider
* security and privacy issues that the IT team must address.

Distributed network

* reduce network costs
* encouraged teleworking , web based applications
* vpns

wan operations

wans standards

Extra info :Zeker, telecommunicatie is het verzenden van informatie over afstand. Het betreft het overbrengen van geluiden, tekst, beelden of gegevens tussen mensen of machines met behulp van technologie

* Modern WAN standards are defined and managed by a number of recognized authorities including the following:
  + TIA/EIA - Telecommunications Industry Association and Electronic Industries Alliance
  + ISO - International Organization for Standardization
  + IEEE - Institute of Electrical and Electronics Engineers
* Layer 1 protocols : electricial mechinanical and operational components needed to transmit bits over a wan , fiber optical protocol standards
  + Synchronous Digital Hierarchy (SDH)
  + Synchronous Optical Networking (SONET)
  + Dense Wavelength Division Multiplexing (DWDM)
  + SDH and SONET essentially provide the same services and their transmission capacity can be increased by using DWDM technology.
* Layer 2 = data enscapulate in to frame
  + Broadband (i.e., DSL and Cable)
  + Wireless
  + Ethernet WAN (Metro Ethernet)
  + Multiprotocol Label Switching (MPLS)
  + Point-to-Point Protocol (PPP) (less used)
  + High-Level Data Link Control (HDLC) (less used)
  + Frame Relay (legacy)
  + Asynchronous Transfer Mode (ATM) (legacy)
* Afbeelding met tekst, schermopname, diagram, ontwerp

  Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, document, Parallel

Automatisch gegenereerde beschrijving

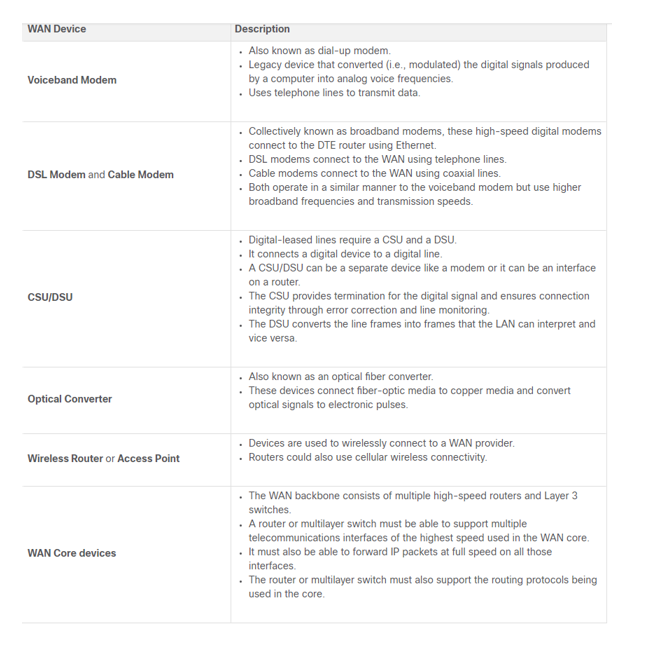
Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Wan devices

Afbeelding met diagram, schermopname, lijn, tekst

Automatisch gegenereerde beschrijving

wZ 

Serial communication :

* Almost all network communications occur using a serial communication delivery. Serial communication transmits bits sequentially over a single channel. In contrast, parallel communications simultaneously transmit several bits using multiple wires.
* Parralel communications has synchronisation problems
* Parallel communication is only limited to short distances
  + used in distances between serves and switches where the distance is short => data centers

circuit switch communication

* dedicated circuit (or channel) between endpoints before the users can communicate.
* a dedicated virtual connection through the service provider network before voice or data communication can start.
* all communication uses the same path
* inefficiencies in circuit usage. For this reason, circuit switching is generally not suited for data communication.



Packet-Switched Communications

* switching segments traffic data into packets that are routed over a shared network
* Packet-switched networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel
* Less expensive
* Latency and jitter
* Packet-switched technology metro ethernet, multiprotocol label switching mpls

Afbeelding met schermopname, diagram, cirkel, ontwerp

Automatisch gegenereerde beschrijving

SDH, SONET, and DWDM

* use fiber-optic infrastructures to transport user data between destinations.
* Fiber-optic cable is far superior to copper cable for long distances
* There are two optical fiber OSI layer 1 standards
  + Shd
  + Sonnet
* Both standards are essentially the same and therefore, they are often listed as SONET/SDH.
* SDH/SONET define how to transfer multiple data, voice, and video communications over optical fiber using lasers or light-emitting diodes (LEDs) over great distances.
* Both standard used in ring network topology
* Data carrying topology using wavelength => DWDM

Traditional WAN Connectivity

Traditional WAN Connectivity Options

Afbeelding met tekst, schermopname, diagram, Lettertype

Automatisch gegenereerde beschrijving

Common WAN Terminology

* Point-to-point lines could be leased from a service provider and were called “leased lines”.
* The term refers to the fact that the organization pays a monthly lease fee to a service provider to use the line.
* There are two systems used to define the digital capacity of a copper media serial link:
  + T-carier vb t3
  + E-carier vb e3
* Advantage leased lines
  + Simplicity
  + Quality
  + Availability
* Disadavantage
  + Cost
  + Limited flexibility

Circuit-Switched Options

* Circuit-switched connections are provided by Public Service Telephone Network (PSTN) carriers.
* Two traditional circuit switched options
  + Pstn : public service telephone network
  + Isdn => intrgrated services digital network
* Lsdn word niet meer gerbuikt

Packet switched option

* Frame relay
* Asynchronous transfer mode

Modern wan connectivity

Modern wans

Afbeelding met diagram, lijn, schermopname, kaart

Automatisch gegenereerde beschrijving

Modern wan connectivity options

Afbeelding met tekst, schermopname, diagram, Rechthoek

Automatisch gegenereerde beschrijving

Packet-Switched :

* Two packet-switched WAN network options are available.
* Advances in Ethernet LAN technology have enabled it to expand into the MAN and WAN areas. Metro Ethernet provides fast bandwidth links and has been responsible for replacing many traditional WAN connectivity options.
* Multi-protocol Label Switching (MPLS) enables the WAN provider network to carry any protocol (e.g., IPv4 packets, IPv6 packets, Ethernet, DSL) as payload data. This enables different sites to connect to the provider network regardless of its access technologies.

Internet-based Broadband

* organizations are now commonly using the global internet infrastructure for WAN connectivity. To address the security concerns, the connectivity options are often combined with VPN technologies.
* Valid WAN network options include Digital Subscriber Line (DSL), cable, wireless, and fiber

Ethernet wan

* Ethernet wan using fiber optic cable
* Ethernet wan services
  + Metro e
  + Eompls
  + Vpls
* Benefits
  + Reduced expenses and administration
  + Easy integration with existing networks
  + Enhanced business productivity

Mpls

* Multiprotocol label switching
* High profromance service provider wan routing technology to interconnect client without regard to access method or payload
* Can enncapsulata all types of protocols including ipv4 and ipv6 traffic
* Mpls router can be customer edge (ce) router, a provider edge (pe) or a internal provider
* Mpls router a label switched routers this means they attach label to packet that are then used bu other mpls router to forward traffic
* Mpls routers use the label to determine the next hop of the packet
* Mpls als provides sercices for qos support , traffic engineering redundancy, vpn

Afbeelding met diagram, lijn, cirkel, schermopname

Automatisch gegenereerde beschrijving