Networking_TutorialYT

Network Engineer / Complete Networking Course

FreeCodeCamp + PaceIT on YT

CompTIA Network+

These notes are from the networking course of freecodecamp on yt. The notes are only made till the "Common network threats" part.

Introduction to Network Devices 1

Layer 1 Devices

The OSI (Open Systems Interconnection) reference model was developed to help disparate devices communicate on networks. Devices may be classified by the level of the OSI model at which they operate.

Analog Modem

The analog modem modulates a digital signal into an analog signal and demodulates the return signal to allow for network communication.

Hub

The hub recieves a network signal on a port and replicates that signal out all of the remaining ports.

Layer 2 Devices

Switch

The switch utilizes an ASIC (Application Specific Integrated Circuit) chip to learn which devices are connected to which ports via the device's layer 2 MAC (Media Access Control) address. When the switch receives network traffic, it will only forward that traffic to the specified MAC address.

Wireless Access Point

The Wireless Access Point (WAP) is used to bridge wireless network segments with wired network segments.

Layer 3 Devices

Multi Layer Switch

The Multi Layer Swtich (MLS) operates at more than just layer 2 of the OSI model. The most common MLS is the layer 3 switch. The ASIC chip is programmed to handle more than just the layer 2 MAC address.

Router

The router is the most common device user to connect different networks together. It utilizes software programming to learn about routes between networks.

Introduction to Network Devices 2

Security Devices

Firewall

Firewalls are the police force of the network. They either allow or deny network traffic based on a set of predefined rules. They may be an appliance or software based.

Intrusion Detection System

An Intrusion Detection System (IDS) will inform a network administrator when malicious actions have occured (they are passive).

Intrusion Prevention System

An Intrusion Prevention System (IPS) is placed inline with network traffic and will take action when malicious

activities are detected.

Optimization & Performance Devices

Load Balancer

A load balancer (aka a content switch or content filter) is a network applicance that will balance requests across multiple devices that contain the same data.

Proxy Server

A proxy server acts on behalf of a client device to fulfill requests to retrieve data It can also be used to limit what requests are fulfilled.

Networking Services & Applications 1

Basics of Virtual Private Network

A VPN connection is used to allow remote sites or users to access a private network and to function as a local segment.

Site-to-Site VPN

A site-to-site VPN connects two sites together.

Remote-Access VPN

A remote-access VPN allows select users to connect, but requires those users to have preconfigured VPN clients installed on their systems.

Host-to-Host VPN

A host-to-host VPN allows users to connect to the private network without the use of VPN client software.

Protocols used by VPN

Internet Protocol Security

IPsec is the most common protocol suite used to secure VPN connections. It works at layer 3 and above of the OSI model.

Generic Routing Encapsulation

GRE is a tunneling protocol that can encapsulate a wide variety of other network layer protocols. It is used in conjunction with IPsec to allow for multicast (one to some) and broadcast (one to many) packet transmissions.

Point-to-Point Tunnelling Protocol

PPTP is an older VPN technology that supports dial-up VPN connections.

Transport Layer Security

TLS is a cryptographic protocol that provides authentication services; it is commonly used in Web based transactions and has largely replaced SSL.

Secure Sockets Layer

SSL is similar to TLS and has largely been replaced by it.

Networking Services & Applications 2

Network Access Services

Network Interface Card

The Network Interface Card (NIC) operates at both layers 2 and 1 of the OSI model. It is what determines what networking protocol a device will use on the network and is responsible for converting the network bits into an electrical signal.

Remote Authentication Dial-In User Service

RADIUS is an AAA (Authentication, Authorisation, Accounting) protocol used to authenticate end users. It has very robust accounting features.

Terminal Access Controller Access Control System+

TACACS+ is a AAA (Authentication, Authorisation, Accounting) protocol used to authenticate end devices. It encrypts all transmissions between devices.

Other Services & Applications

Remote Access Service

RAS is a description of the combination of software and hardware required for a remote access connection (its not a protocol).

Web Services

Web servies are used to allow disparate software or platforms to communicate. They will usually translate communication into an XML (Extension Markup Language) format that most software can understand.

Unified Voice Services

Unified Voice Services is a description of the combination of software and hardware used to bring voice communication into a network.

Dynamic Host Configuration Protocol (DHCP) in the network

Static vs Dynamic IP addressing

Internet Protocol (IP) configurations can be static or dynamic.

Static IP addressing

In a static configuration, an administrator supplies all of the required IP information to each device that requires it in a network.

Dynamic IP addressing

In a dynamic configuration, an administrator configures a DHCP server to automatically distribute the required IP configuration information upon request.

How DHCP works?

A device sends a discovery packet. A DHCP server responds with an offer packet (letting the device know that the DHCP server has the required information). Upon receipt of the offer packet, the device sends a request packet (requesting the proper IP configuration). When the DHCP server gets the request packet, it responds with all of the information in an acknowledgement packet.

Components and processes of DHCP

DHCP uses User Datagram Protocol (UDP) ports 67 and 68 to provide the IP configuration to a Personal Computer (PC). The IP address comes from a scope (range) of addresses configured by the administrator. The administrator can reserve a pool of addresses. Options include: default gateway, DNS servers, time servers, and other options. Addresses are leased and leases expire; however, a device can request the same IP address again.

DHCP Relay

A DHCP relay can be used when a DHCP server doesn't reside on the local network segment.

Introduction to the Domain Name System service

DNS servers

DNS is used to map human friendly names to IP addresses. It utilizes a set of servers (root, TLD, and local) to resolve the Fully Qualified Domain Name (FQDN) to the right IP address.

Responses

Responses can be authoritative or non-authoritative.

DNS records

A

'A' record maps hostnames to IPv4 addresses.

AAAA

'AAAA' record maps hostnames to IPv6 addresses.

Canonical Name

CNAME record maps canonical names to hostnames.

Pointer

PTR record points to canonical names.

Mail Exchanger

MX record points to the email server responsible for handling the email for a given domain.

Dynamic DNS

Dynamic DNS (DDNS) allows for lightweight adjustments to the local DNS databse. It is useful on networks that don't use static IP addresses. DDNS updating is used to automatically update DNS records without having to manually input the information.

Introduction to Network Address Translation

Purpose of NAT

NAT solves the problem of how to route non-routable IP addresses. Private IP addresses cannot cross public IP networks, limiting private IP networks to being local only. NAT transforms the private IP address inot a routable

public IP address, which allows access outside of the local network.

How NAT works?

There are two main categories of NAT - static and dynamic.

Source Network Address Translation

In SNAT, each private IP address that is allowed access outside of the local network is assigned a specific public IP address that is used for that access.

Destination Network Address Translation

In DNAT, when a device requres access outside of the local network, it is dynamically assigned a public IP address from a pool of available addresses.

Port Address Translation

PAT was developed as a method of extending the capabilities of DNAT.

NAT's private IP addresses

NAT uses specific terminology to refer to IP addresses: inside local, inside global, outside global and outside local.

Inside Local

Inside Global

Outside Local

Outside Global

Wide Area Network Technologies 1

One of the best indication of a WAN is if the infrastructure is not owned by a single entity.

Public Switched Telephone Network

The PSTN is one of the most widely used WAN infrastructures. The PSTN can be used to carry analog traffic through a dial-up connection or digital traffic through ISDN or xDSL connections.

Integrated Services Digital Network

Digital Subscriber Line

Broadband Cable

Cable companies can provide broadband cable connections to customers. These are capable of carrying voice, data and television - all through the same cable. The signal is formatted at the headend and delivered to the distribution network to be sent on to the end users. The end users all share the bandwidth of the distribution network.

Fiber

Fiber is a fast, high bandwidth WAN technology that uses light to transmit voice and data down a fiber optic cable. It is capable of achieving multiple gigabit transmission levels.

SONET & SDH

SONET (Syncrhonous Optical Network) (in the U.S.) and SDH (Synchronous Digital Hierarchy) establish the base rates of the optical carrier (OC) levels.

DWDM & CWDM

Dense Wavelength Division Multiplexing (DWDM) and Coarse Wavelength Division Multiplexing (CWDM) are the methods used to multiplex multiple OC levels into a single fiber optic cable.

Wide Area Network Technologies 2

GSM/CDMA WAN Connections

Global Systems for Mobile Communication (GSM) and Code-Division Multiple Access (CDMA) are the two main methods of connecting cellular devices to cellular networks and they are not compatible. True WAN cellular connections were not available until High Speed Packet Access (HSPA+), which is a stop gap measure between 3G & 4G networking. The emerging standard for cellular networking is 4G, which currently consists of Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX).

WiMAX WAN Connections

WiMAX was originally designed as a last mile solution for areas in which DSL and cable were not available. It utilizes microwave signals between line-of-sight relay stations to deliver broadband traffic to a fixed loation. It is compatible with LTE so it is considered a 4G technology. It can span significant geographic distances.

Satellite WAN Connections

Satellite uses microwave radio transmissions as a method of transmitting data over the air. Uses microwave radio relays and satellites to span large distances that are still line of site. These vast distances often lead to latency in the transmissions.

Wide Area Network Technologies 3

Metro Ethernet WAN Connections

In a metro Ethernet environment, the service provider supplies the customer with what appears to be an Ethernet connection to the network. While the customer views the connection as being Ethernet, the service provider may use a variety of different WAN technologies, depending on the level of service required.

Leased Line WAN Connections

A leased line is a dedicated connection between two end notes that the customer leases from a telecommunications company. Usually, it will either utilize Plain Old Telephone Service (POTS) or a fibre optic connection.

T-Carrier Line

A T-carrier line is composed of 24 DS0 channels, each capable of handling 64 kbps. The 24 DS0 channels make up a single DS1 line.

Optical Carrier Levels

Optical carrier levels are established by SONET and SDH and may use CWDM or DWDM to increase capacity on a cable.

Common Standards

T-Carrier Lines

The most common T-Carrier Lines are T1 (1.544 mbps) and T3 (44.736 mbps). The T3 line is composed of 28 T1 lines.

E-Carrier Lines

The most common E-Carrier lines are the E1 (2.048 mbps) and the E3 (34.368 mbps). The E3 line is composed of 16 E1 lines.

Optical Carrier Lines

The two most common Optical Carrier Lines are the OC1 (51.48 mbps) and the OC3 (155.52 mbps).

Wide Area Network Technologies 4

Circuit Switched vs Packet Switched Networks

A circuit switched network involves a dedicated point-to-point connection between two nodes. They are commonly used with leased line networks. In a packet switched network data is broken down into smaller packets and routed through the network using the destination address the data may take different paths to reach the address.

Frame Realy vs Asynchronous Transfer Mode

A packet switching technology is one in which the network packets can be different sizes. Frame relay may be set up to mimic a circuit switched network. ATM (Asynchronous Transfer Mode) Technology uses a fixed cell size (53 bytes) to quickly move network traffic. While ATM is a fast Technology it doesn't use the available bandwidth efficiently due to the fixed size of all the cells.

Multiprotocol Label Switching

MPLS (Multi-Protocol Label Switching) is a WAN packet switching technology that has gained in popularity because of its scalability and protocol independence it can be used to replace both frame relay and ATM or it can be used in conjunction with either or both of those technologies it uses LERs (Label Edge Routers) to insert MPLS labels into packets and LSR (Label Switching Router) to route the packets to their destinations.

Network Cabling 1

Twisted Pair Cabling

Twisted pair cabling is the modern LAN (Local Area Network) standard. It is composed of four pairs of color coded wires where each pair of wires is twisted together to reduce interference. It may contain extra shielding to further reduce interference in some cases a plenum grade cable may be called for by building codes the most common types are: straight through, crossover and rollover cables.

Twisted Pair Network Connectors

(RJ = Registered Jack, DB = D-Subminiature Connectors)
The RJ11 is a modular six position four contact (6P4C) connector commonly used for telephony. The RJ45 is a modular (8P86) connector that is used to carry network traffic. The RJ48C is a modular (8P86) connector that is commonly used to terminate a T1 line. Punchdown blocks are used to terminate and distribute network runs of twisted pair wires. The DB9 and DB25 may be used for serial communication between nodes.

Categories of Twisted Pair

(Category = CAT)
CAT3 can achieve speeds of 10 MBPS. CAT5 can achieve speeds of 100 mbps, CAT5e can achieve speeds of 1000 mbps, CAT 6 can achieve speeds of 10 gbps (over a max of 55m), and CAT6a can achieve speeds of 10 gbps.

Network Cabling 2

Coaxial Cabling

Coaxial cabling is composed of a central conductor covered by an insulating sheath, covered by a foil or metal mesh sheath, covered by an outer insulating layer. RG58 is no longer found in the modern network. RG59 is used to provide a short distance broadband connection between two devices. RG6 is the most commonly used grade of cable used by cable companies to connect to the cable modem.

Fiber Optic Cabling

Fiber optic cabling is expensive and can be difficult to work with but resists all forms of EMI (Electromagnetic Interference) and can span long distances. The grade of connector can influence the quality of the signal. Fiber optic cabling is classified by its type of transmission as either being MMF (Multimode Fibre) or SMF (Single Mode Fibre); currently there are four common types of connectors SC (Square Connector), ST (Straight Tip), LC (Lucent Connector) & MTRJ (Mechanical Transferred Registered Jack).

Network Cabling 3

Media Converters

Often there will be a need to transition from one type of network cabling to another. Media converters make that transition possible resulting in a cohesive network. Common media converters are SMF to Ethernet, MMF to Ethernet, SMF to MMF and fiber to coaxial cabling.

Cabling Tools

Each technician will need to determine the types and quality of tools in his or her toolbox. Common network cabling tools include crimpers, strippers, punch down tools, and cable testers. Not quite so common or practical for most technicians are the TDR (Time Domain Reflectometers) and the OTDR (Optical Time Domain Reflectometers)

Network Topologies

What is a topology?

A map that can be used to describe the signal path of the physical layout of a network. The logical topology will describe the signal path while the physical topology is more of a wire schematic.

Peer-to-Peer vs Client-Server vs Hybrid Topology

In peer-to-peer networking there is no central control of network resources. Each node determines what it will share and what it will not share. In client server networking there is central control of shared network resources with a server controlling access. A network can have aspects of both and this is considered a hybrid topology.

Network Topology Models

Ethernet networks are logical bus networks regardless of the physical layout.

Bus

Bus= signal goes end-to-end.

Ring

Ring = bus with the ends connected.

Star

Star = nodes radiate out.

Mesh

Mesh = multipath.

Point-to-Point

Point-to-point = direct connection.

Point-to-Multipoint

Point-to-multipoint = central control.

MPLS

MPLS = a topology used to improve QoS (Quality of Service) and network traffic flows.

Network Infrastructure Implementations

Design vs Function

A network can be described by its design or by its function. When describing the design (eg. bus, star, point-to-point) the topology is actually being described. When describing the function (eg. LAN, WAN, SCADA) of a network, it is actually the category or infrastructure implementation that is being discussed.

Categories of networks

Local Area Network

The LAN (Local Area Network) spans a small area, like a building.

Metropolitan Area Network

While there is not a distinct line between the LAN and the MAN, the MAN (Metropolitan Area Network) is larger than the LAN.

Wide Area Network

WAN (Wide Area Network) span large geographic areas. As a rule, if the infrastructure is owned by one entity, it is not a WAN.

Personal Area Network

PANs (Personal Area Network) are very small, low powered networks that tend to only span two devices.

Supervisory Control And Data Acquisition Network

A SCADA (Supervisory Control And Data Acquistion) network is a special purpose network used to control equipment and processes across multiple industrial sites.

Medianet

A medianet is a purpose built infrastructure designed and implemented specifically to handle voice and video traffic.

Introduction to IPv4 1

Purpose of IP Addressing

IP addressing is logical in nature so it can be easily changed. It provides the means of identifying the pathways between networks and nodes.

IPv4 Address Properties

IPv4 is made of a 32-bit binary number (base 2). There are over four billion possible combinations.

Subnet Mask

A subnet mask is used to allow for the identification of the network and node portions of the IP address.

Introduction to IPv4 2

Classes of IPv4 Addresses

Based on numerical range

Classes consist of A, B, C and D. All have a defined subnet mask, except for class D addresses. They are very structured and rigid and don't allow for much flexibility.

Class A

Class B

Class C

Class D

Others

Automatic Private IP Addressing

An APIPA address is a special address that denotes the failure of DHCP.

Public IP Addresses

Public addresss are routable, private addresses are not. There are very specific ranges of addresses available in the private space.

Private IP Addresses

Public addresss are routable, private addresses are not. There are very specific ranges of addresses available in the private space.

Classless IPv4 Addressing

Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR) remove shte class structure from addresses, creating more flexibility and efficiency in design and utilization. It allows for subnetting of addresses.

Subnetting IPv4 Addresses

Subnetting involves taking the network address space that is available and creating small pieces. It is used to create flexibility and security within a network.

Introduction to IPv6

IPv6 Address Structure

The IANA (Internet Assigned Numbers Authority) developed IPv6 as a long term replacement to IPv4. It is a 128-bit binary addressing scheme that provides 340 X 10^36 possible unique addresses. It is represented by eight sets of colon separated hexadecimal numbers (each set representing 16 bits). IPv6 is capable of auto-configuration through the use of NDP (Neighbour Discovery Protocol).

DHCPv6

DHCPv6 is only used in certain specific network configurations.

IPv6 Network Transmissions

By implementing a dual stack configuration or using 6to4 tunnelling, IPv6 can be used in conjunction with IPv4.

Unicast

Unicast is one-to-one communication (one device sending to a specific device).

Multicast

Multicast is one-to-few communication (one device sending to a registered group).

Anycast

Anycast is one-to-closest communication (one device sends to a specific IPv6 address, which has been assigned to multiple devices and the closest one receives the packet).

Special IP networking concepts

Media Access Control Address

All network devices come with MAC address (also called the physical address or burned-in address) which are used by Layer 2 network devices to deliver packets to the correct nodes on the network. The MAC address is composed of the OUI (Organzational Unique Identifier), which is assigned by IEEE (Institute of Electrical and Electronics Engineers) and the EUI (Extended Unique Identifier), which is assigned by the manufacturer. IPv6 requires an EUI-64 format address.

Collision Domains vs Broadcast Domains

Ethernet networks utilize CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to alleviate network traffic collisions. Collision domains are areas of the network in which network traffic can occur. Collision domains are broken up by Layer 2 and higher devices. Broadcast domains are areas of the network that will receive broadcast network traffic. IPv6 uses multicast transmissions in place of broadcasts.

Types of Network Transmissions

IPv4 Transmissions

IPv4 uses unicast (one-to-one communication), multicast (one-to-few communication), and broadcast (one-to-all communication) network transmissions.

Unicast

unicast (one-to-one communication)

Multicast

multicast (one-to-few communication)

Broadcast

broadcast (one-to-all communication)

IPv6 Transmissions

IPv6 also uses unicast and multicast transmissions. In addition, IPv6 uses anycast (one-to-closest) network transmissions to deliver network traffic to the nearest device that has a specific IPv6 address, which has been assigned multiple devices.

Unicast

unicast (one-to-one communication)

Multicast

multicast (one-to-few communication)

Anycast

anycast (one-to-closest) is used to deliver network traffic to the nearest device that has a specific IPv6 address, which has been assigned multiple devices.

Introduction to Routing Concepts 1

Purpose of Routing

The purpose of routing is to connect different networks together logically for communications purposes and to allow for network data traffic to reach remote networks. Most often, routing protocols are used to build dynamic routes between networks.

Basic Routing Concepts

Static Routing

Static-Routing involves administratively configured routes between networks - the administrator must manually make any changes.

Dynamic Routing

Dynamic routing involves protocol configured routes between networks - the protocols determine when and how to make routing changes.

Default Route

A default route is the next interface or next hop that a router sends a network packet to when no known route exists.

Routing Table

The routing table is the administratively configured or protocol configured table of routes to all known networks.

Loopback Interface

A loopback interface is a logically assigned interface used to ease the administrative management of a router.

Routing Loop

A routing loop is a possible problem between interconnected routers where network traffic keeps circling until some system or mechanism breaks the cycle.

Introduction to Routing Concepts 2

Routing Metrics

Routing Protocols use metrics to determine which route is the best route to use to reach remote networks. Routing protocols can use the same metrics, but will use different algorithms to populate their routing tables. Common metrics include:

Hop Count

Maximum Transmission Unit

Bandwidth

Latency

Administrative Distance

Routing Aggregation

Without some planning, routing tables can become large and inefficient. Route aggregation is a method of summarizing routes to different networks through the use of CIDR (Classless Inter-Domain Routing). Care and caution must be used when non-contiguous networks are present.

High Availability

Network Technicians use high availability techniques in an effor to remove single points of failure from networks. Hot Standby Router Protocol (HSRP) & Virtual Router Redundancy Protocol (VRRP) are examples of high availability techniques that are implemented to reduce the changes that a single router going offline will create a problem for the network.

Introduction to Routing Protocols

Interior vs Exterior Gateway Protocols

IGP (Interior Gateway Protocol) routing protocols are used with autonomous networks (networks under the control of a single organisation). BGP (Border Gateway Protocol) routing protocols are used between non-autonomous networks. Some IGP protocols use an AS (Autonomous System) number to help determine which networks can connect with each other.

More Routing Concepts

IGP (Interior Gateway Protocol) and EGP (Exterior Gateway Protocol) routing protocols can be broken into three types:
distance-vector protocols, link state protocols, and hybrid protocols. Their classification is determined by how they operate. The next hop is the next router in the path of a route. The routing tables is a database of all known

routes from the perspective of the router. Convergence is when the network has reached a steady state.

Routing Protocols

RIPv2

RIPv2 (Routing Information Protocol Version 2) is a distance-vector routing protocol that only cares about the number of hops between the source and destination.

OSPF

OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) are link state routing protocols that use the Dijkstra algorithm. BGP (Border Gateway Protocol) is a hybrid path-vector routing protocol and is considered the routing protocol of the Internet. EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector (hybrid) routing protocol developed by Cisco.

IS-IS

OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) are link state routing protocols that use the Dijkstra algorithm.

BGP

BGP (Border Gateway Protocol) is a hybrid path-vector routing protocol and is considered the routing protocol of the Internet.

EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector (hybrid) routing protocol developed by Cisco.

Basic Elements of Unified Communications

Unified Communications

UC is the set of products and services used to facilitate communication across different devices and media (eg.,

transforming a voice mail message into an email). UC servers are specialized servers used to implement UC solutions in the workplace. UC gateways are devices used to translate between different signalling methods (eg., a VoIP gateway translating an analog PSTN connection into a digital network signal).

Unified Communications Concepts

Presence is an indicator that is used to communicate the willingness or ability of someone to receive communication. A presence service is used to track users across multiple devices and to deliver communication to the appropriate location or device. QoS (Quality of Service) is set of techniques used to manage network traffic and is often implemented to improve UC.

Voice over IP

SIP

VoIP is one of the most commonly implemented UC solutions. VoIP uses SIP (Session Initiation Protocol) to establish and tear down communication sessions.

RTP

During the actual communication session, RTP (Real-time Transport Protocol) is used as the transport mechanism for the communication. RTP helps to provide QoS to the end points.

Virtualisation Technologies

Hypervisors and Virtual Machine Managers

Depending on the source, a hypervisor and VMM (Virtual Machine Manager) may be considered to be the same thing. Others differentiate the two this way: a hypervisor doesn't require a host OS in order to function and serve up VMs, while a VMM requires the use of an underlying host OS in order to function.

Components of Virtualisation

Virtual Machine

Virtual Machines can be created to fulfill almost any function in the modern network (eg, virtual desktops, servers, routers & switches).

Virtual Networks

Virtual networks may be completely self-contained, or a connection may be created between the host system's physical NIC (Network Interface Controller/Card) and a virtual networking device to allow network traffic to pass through system.

Software Defined Networking

SDN is an emerging technology that is being used to allow network administrators to dynamically adjust network performance from a single interface. This eliminates the need for the administrator to log into each network device that needs to be adjusted in order to achieve the desired performance.

Storage Area Networks

Justification for SAN

The reduction in cost of storage and the increased desire to access data at anytime from anywhere has led to an increase in the demand for data storage. The SAN is a solution to the data storage needs of the modern era. SANs are scalable, can lead to increased data availability, and can also be used to optimize networking performace.

SAN Technology

SAN vs NAS

A SAN is a network of storage capacity, while a NAS (Networking-Attached Storage) is a data storage device (or devices) that is attached to a network. Multiple NAS devices may be found within a SAN.

Fibre Channel

Fibre Channel (FC) uses FCP (Fibre Channel Protocol) as the transport protocol to connect SANs and to transmit SCSI (Small Computer Small Interface) commands and processess to occur over long distances.

Jumbo Frames

Jumbo frames can be used to increase data throughput by allowing payloads of upto 9000 bytes.

Basic Cloud Concepts

Cloud Classifications

The use of cloud computing means that network resources are provided virtually instead of physically. This can lead to a very dynamic and fluid computing environment. The type of cloud deployed can be classified in one of four ways.

Public

Private

Hybrid

Community

Types of Cloud Computing

The highly configurable nature of cloud computing has led to several different types of cloud computing.

Software as a Service

In SaaS, only a software package is provided (which is usually run from within a web browser).

Platform as a Service

PaaS provides development platform that is usually used in the creation of software packages.

Infrastructure as a Service

With IaaS, the user configures the virtual network resources that will be used - from virtual servers all the way down to the software packages.

Implementing a Basic Network

Plan the Network

A network plan is vital when implementing any network more complicated than the most basic one. At the minimum the plan should include a list of requirements, a network design, compatibility considerations, a list of internal and eternal connections, a list of where equipment will be placed, and a means of implementing security.

Configure the Network

Configuration considerations include IP address, assignment, MAC filtering, DMZ (Demilitarized Zone) configuartion (when required), firewall placement and configuration, and router configuration. For wireless networks, additional configuration considerations include: SSID (network's name), SSID broadcast type and encryption method.

Wired Networks

IP Address Assignment

MAC Filtering

DMZ Configuration

Firewall Placement & Configuration

Router Configuration

Wireless Networks

IP Address Assignment

MAC Filtering

DMZ Configuration

Firewall Placement & Configuration

Router Configuration

Service Set IDentifier

SSID is the network's name

SSID Broadcast Type

Encryption Method

Analyzing Monitoring Reports

Baselines

Baselines are used to establish what network performance should be. Periodic tests should be conducted against the baselines to determine if they have changed.

Functions benefitting from baselines

Functions that might benefit from having a baseline include: network device CPU utilization, network device memory utilization, bandwidth utilization, storage utilization, and wireless channel utilization

Network Device CPU Utilization

Network Device Memory Utilization

Bandwidth Utilization

Storage Utilization

Wireless Channel Utilization

Reports

Log files can accumulate data rather quickly. Admins can help manage the growth through setting the proper reporting levels. Log reports do need to be reviewed and should be archived. Grahing log data can give a visual reference that makes it easier to sport problems. Any interface link status other than u and up indicates that there may be an issue. Problems can still occur on a network interface, even when link status is up and up.

Issues if Status is up & up

Issues that can occur include: speed and duplex mismatch, discarded and dropped packets, and interface resets.

Speed & Duplex Mismatch

Discarded & Dropped Packets

Interface Resets

Network Monitoring 1

The "why" of Networking Monitoring

As network admins are responsible for keeping the network up and running, they hate to be surprised by network failures - especially ones they could have foreseen and, therefore, have forestalled. To prevent this, they will deploy a variety of tools to keep track of the network's health and behaviour.

Tools for Monitoring the Network

Log Files

Log files are an important tool that network admins can use to track how their network and systems are running. Almost all OS are capable of generating log files, which are usually a more passive and after-the-fact type of monitorying.

Event Viewer

Event Viewer is a Microsoft tool used to track and organize log files.

Syslog

Syslog was created in the 1980s to provide a method of communication between devices that would no normally communicate. Syslog events are rated on a scale of zero to seven, based on the severity of the event (with zero being the most sever).

Simple Network Management Protocol

SNMP (Simple Network Management Protocol) is a protocol that takes a more active approach in monitoring the network and systems. With SNMP, a trap is set on a device. When the trap is tripped, a message is sent to the NMS (Network Mangement System), which stores the even in the MIB (Management Information Base). Depending on the severity, a message may be sent to an administrator via SMS (Short Message Service) or email.

Network Monitoring 2

Active Network Monitoring Tools

Port Scanners

Port scanners are used to scan for unsecured ports and protocols. The information gathered by port scanners is used to harden networks and make them less vulnerable to security breaches.

Packet Sniffers

Interface monitoring evaluates network traffic at the packet level. Packet sniffers can help to identify issues on the network that can then be mitigated.

Wireless Monitoring Tools

Wi-Fi Analyzer

A Wi-Fi analyzer is similar to a packet-sniffer, but checks wireless network packets instead. Analyzers can also identify which RF (Radio Frequency) channels are in use. The analyzer can help to identify wireless networks, even ones that are hidden.

Wireless Survey Tools

Wireless survey tools are used to help design efficient and secure wireless networks.

Environmental Monitoring

A network's function and health can be affected by environmental factors.

Power Monitors

Power monitors are used to evaluate the electrical supply being delivered to the system.

Heat & Humidity Monitors

Heat and humidity monitors are used to help maintain the correct levels of heat and humidity.

Supporting Configuration Management 1

S

Configuration Management

Configuration Management (CM) is a discipline that is used to evaluate, coordinate, approve, deny or implement change in or to an IT system. In the CM process, documentation is used to help evaluate and plan proposed changes.

Documentation

Documentation is used to help in asset management, network maintenance, and vendor evaluations.

Policies

Policies are a set of guidelines established by mid to upper management.

Procedures

Procedures are a set of documents used to determine how policies will be implemented.

Asset Management Documentation

Asset management documentation is a broad category of documents that provide detailed information on the assets that are present.

Physical Network Diagrams

Physical network diagrams detail the physical strucutre of the network.

Logical Network Diagrams

Logical network diagrams detail the specifics of the network (eg, ports, protocols, IP addresses, and VLAN (Virtual Local Area Network) configurations).

Vendor Documentation

Vendor documentation is a broad category of documents that are used in vendor processes.

Supporting Configuration Management 2

Backups

Backups play an important role in any CM (Configuration Management) system. Backups are used to recover from failed system components or loss of data. Backups may be full, incremental, or differential in nature. Each has its

own advantages and disadvantages. Network devices should have their OS and configuration files backed up as well.

Bring Your Own Device

BYOD allows employees to bring in and use their favorite devices on an organization's network. Since IT departments are responsible for the IT security of networks, this has led to some concerns. NAC (Network Access Control) is implemented in order to help ensure that BYOD policies do not introduce problems to the network. NAC screens devices for their suitability to join and use network resources.

The Importance of Network Segmentation

OSI Model and Segmentation

Segmentation is taking a single system or network and breaking it inot smaller discrete units. Network segmentation can occur at various levels of the OSI model. At layer 1, the segmentation is physical (completely separate cable runs and network hardware). At layers 2 & 3, the segmentation is logical (the segmentation occurs through programmable configurations).

Reasons for Segmentation

There are many reasons for segmenting networks and systems, including compliance, network performace optimization, creating high performance networks, security, creating honeynets, and securing and isolating SCADA systems.

Applying Patches & Updates

Patches & Updates

Modern computing systems contain million of lines compex code, leading to the need for patches, updates and hotfixes. The update process can be automated in most cases, but it is wise to test updates before deploying to a production environment.

Patches

A patch is a small section of code used to fix a problem.

Updates

An update is larger than a patch and often includes increased functionality.

Hotfixes

A hotfix is usually smaller than patch and is used to fix a very specific problem.

Upgrading vs Downgrading

While it can be desirable to have all operating systems and software packages up to date on patches, updates, and hotfixes, sometimes this process can introduce new problems into the computing environment. If this happens, it can lead to the need to downgrade a system to a previous stable version. Administrators need to keep backups of all software and configuration files in order to facilitate the downgrade process.

Configuring Switches 1

Unmanaged vs Managed Switches

Switches are layer 2 devices used on networks to move frames (data) from source to destination based on MAC addresses. Unmanaged switches are simple and don't provide a method for configuring their operations. Managed switches can be configured through the command line or some other interface. SNMP (Simple Network Management Protocol) can be used with managed switches to ease the management process.

Spanning Tree Protocol

A switching loop can occur on networks when there are redundant paths between nodes. DEC (Digital Equipment Corporation) created STP (Spanning Tree Protocol) as a means of preventing switching loops from occurring on networks. STP defines five port states: disabled, blocking, listening, learning, and forwarding. STP can take upto 50 seconds to reach convergence. The IEEE (Institute of Electrical and Electronics Engineers) version of STP is 802.1d. RSTP (Rapid Spanning Tree Protocol) (802.1w) was created to decrease the convergence time to approximately five seconds. RSTP defines three port states: discarding, learning and forwarding.

Configuring Switches 2

Installation Considerations

Planning for a managed switch environment can save on time and frustration. Some installation considerations include: the creation of VLANs; in-band and out-of-band switch management, including establishing a default gateway address; user settings; and AAA settings if required.

Configuring the Switch Port

An administrator also needs to consider the settings for each individual port on a switch. Some of these considerations are the speed and duplex used on the port, the VLAN assignment for the port, which ports will handle 802.1q trunking, if bandwidth could be increased by using LACP (Link Aggregration Control Protocol), and how any PoE or PoE+ (Power over Ethernet, Power over Ethernet Plus) ports are available to be used to power devices.

Wireless Local Area Network Infrastructure 1

Introduction to Wireless Network Standards

The IEEE 802.11 standards are the specifications that establish how wireless communications can occur on a network. The 802.11 standards require that specific RF bands and CSMA/CA technology can be used. The standards have evolved over time and include : 802.11b, 802.11a, 802.11g, 802.11n and 802.11ac. Beaforming was introduced with 802.11n.

Antenna Technology

Antennas are used to send and receive RF signals. They may be on omnidirectional or unidirectional in design. Antenna type and placement will have an impact on WLAN performance. MIMO (Multiple Input Multiple Output) uses up to 4 antennas to provide up to 4 spatial streams. MU-MIMO (Multiple User - MIMO) can use multiple antennas and transmitters to spread a signal over upto 8 spatial streams.

Wireless Access Points

The WAP is a foundational component of the WLAN. It can create an entry point to the more traditional wired network, or it can be used on its own. It commonly uses the unlicensed RF to send and recieve network traffic. SOHO APs may have a router built into them. WAPs may be used to bridge wired networks together. In larger wireless environements, wireless controllers are used to seamlessly transfer devices from AP to AP.

Wireless Local Area Network Infrastructure 2

Basic WLAN Topologies

Ad Hoc Network

In an ad hoc network, wireless devices connect without an AP, using an IBSS (Independent Basic Service Set).

Infrastructure Network

In an infrastructure network, one or more WAPS (Wireless Access Point) control access to the network through a BSS (Basic Service Set).

Mesh Network

A mesh network is a type of infrastructure wireless network that uses multiple APS to seamlessly provide network coverage over a larger area through the use of an ESS (Extended Service Set). As device density increases, more WAPS can be added to distribute the load.

WLAN Concepts & Terms

WAPS send out a beacon that contains the SSID (the network name). Hiding the SSID doesn't stop the beacon from being broadcast and is not an effective security measure. Goodput is a measure, in bytes per second, of actual application data that can be transmitted. The closer to the AP that a wireless device gets, the stronger the signal. Site surveys and heat maps can be used to set up efficient wireless networks and to pinpoint problem areas.

Risk & Security Related Concepts

The Big Picture of Recovery

Organizations should establish and enforce standards and policies. These will help to mitigate any risks. DRPS (Digital Risk Protection Services) are developed and used to help recover from a disaster. A BCP (Business Continuity Plan) is a sub-element of a DRP (Disaster Recovery Plan). They identify systems and components that are mission critical to an organization and create plans to mitigate the loss of those identified elements.

Concepts & Terms

A single point of failure is when there is a single point where a failure would create business discontinuity. Network administrators strive to remove them from their systems. A UPS (Uninterruptible Power Supply) is used to mitigate power issues. First responders are the people who first notice and respond to security issues. Ideally, the first responder will have been properly trained. A data breach is any unauthorized access to an organization's data. User awareness and training is used to mitigate risks associated at the user level. Penetration testing is the review of a whole system looking for weaknesses that can then be hardened. Vulnerability scanning is usually an automated process that looks for weaknesses in networks so that any holes can be plugged.

Common Network Vulnerabilities

Vulnerabilities Associated with Unsecure Protocols

Security is never a completed task. It is always an ongoing concern. Administrators can take steps to reduce their exposure to known
vulnerabilities. Some known vulnerable protocols include: Telnet, SNMP v.1 and v.2, FTP, TFTP (Trivial File Transfer Protocol), HTTP, and SLIP (Serial Line Internet Protocol).

Vulnerable Network Practices

Unpatched and legacy systems are vulnerable to exploitation. An open port is a hole in the security of the system. All unused ports should be closed. It is possible to exploit running services, so all unnecessary services should be disabled. Administrators should know which applications send credentials in clear text and take steps to reduce the security risk posed by them. Unencrypted communication channels are subject to interception; a review of all channels should be conducted to reduce this vulnerability. All wireless communications channels should be encrypted. It is possible to intercept communication by capturing and analyzing RF emanations; TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) is a set of specifications that reduces this vulnerability.

Common Network Threats 1

Inside Jobs or Threats

Given the nature and purpose of networks, it can be difficult to make them secure. Common threats that come from within the network itself are: malicious employees, compromised systems, social engineering, ARP (Address Resolution Protocol) cache poisoning, protocol or packet abuse, man-in-the-middle attacks, and VLAN hopping.

Outside Threats

Of major concern to network security personnel are zero day attacks (the exploitation of previously unknown vulnerabilities) and it is imperative that they keep current with what is being developed. Other outside threats include: brute force attacks, spoofing attacks, and session hijacking.

Common Network Threats 2

Outside Threats

Many network security threats fall into more than one category. A very common and broad category of threats is DOS (Denial of Service). There are many types of DoS threats, including traditional Dos, permanent DoS, friendly or unintentional DoS, DDOS, reflective DoS, and Smurf attacks.

Wireless Network Threats

WPS (Wireless Session Protocol) creates an easy method of placing security on a wireless network, bu it also creates a vulnerability in the network. Threats that face wireless networks include war driving or chalking, WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) cracking, rogue access points, and evil twin attacks. Bluetooth networks are also vulnerable to Bluejacking and, possibly, Bluesnarfing.