CCNA Summary

CCNA Routing & Switching *200-120*

Understanding Networks and their Building Blocks

What is a network

A network is nothing more than a collection of interconnected devices. A network is a tool to decrease cost, time, and effort to increase productivity of people. For example by sharing files between offices a company can share data between them is real-time. Networks reduces cost by sharing printers and other divices between multiple clients.

To connect to a network you'll need a **Network Interface Card (NIC)**, this connects to a network via a cable (e.g. Ethernet). A NIC handles layer 1 and 2 (physical and network), the other layers are deligated to software layers in the layers above layer 2.

Hubs and Switchers

To connect more than two devices with eachother you need to use a *Hub* or a *switch*.

A hub has two mayor disadvantages over a switch:

- A hub repeats the information of one host to all other connected hosts. Even if the message is only meant for one other client.
- A hub can process only one message at a time. If multiple clients send a message at the same time a collision occurs. This collision is called a collision domain (all clients connected to one hub share the same collision domain)

Switches don't have a collision domain, which makes it a more efficient and faster device for routing messages on a network. So you cloud say that a switch breaks up a collision domain.

Clients can communicate via three ways over the network.

- **Unicast** A host sends a message to one other host on the network.
- **Broadcast** A host sends a message to all other hosts on the network.
- **Multicast** A hsot sends a message to a couple of hosts on the network.

All hosts connected to a network are in the same **broadcast domain**, which means that a broadcast message will get picked up by all connected hosts in the broadcast domain. Really large networks can have problems with to many broadcasts. A **router** breaks up broadcast domains. Routers seperate networks from eachother and do not allow broadcasts between those networks.

Besides breaking up broadcast networks routers have other essential functions for making multiple interconnected networks possible:

- **Packet Switching** Just like a switch, routers switch packets between networks.
- **Connect Networks** Routers allow connecting networks with eachother.
- **Path Selection** Routers can learn about connected networks and pick the best path to send messages between networks.
- **Packet Filtering** Routers can drop packets based on rules set by a network administrator.

Networking Types

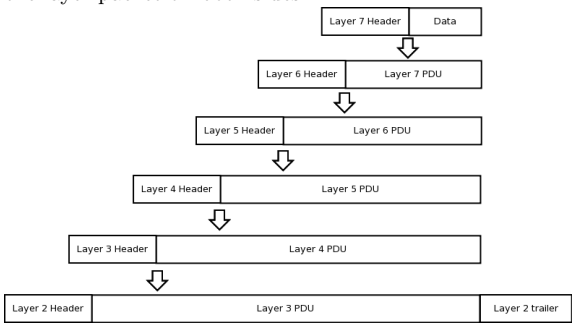
There are two important types of networks: **Local Area Network (LAN)** and **Wide Area Network (WAN)**. LANs are smaller networks most of the time, you'll find them in your home, at work, and at school. They cover a small area like a floor or a building. They can transfer a large amount of data. WANs cover areas like cities, countries, or continents, they connect LANs across areas they cover.

OSI Reference Model

The OSI layer

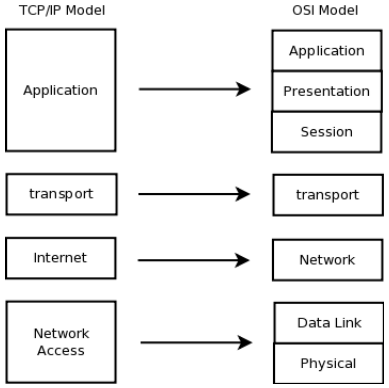
- **Host layer**
  - **Application layer** Protocols for communication with applications.
  - **Presentation layer** Formatting, compression, and encryption/decryption.
  - **Session** Managing of sessions.
  - **Transport** Reliable transmission of data segments between points on a network.
- **Media layer**
  - **Network** Structuring and managing a multi-node network (addressing, routing, traffic control).
  - **Data link** Reliable transmission of data frames between two nodes
  - **Physical** Transmission and reception of raw bit streams over a physical medium.

Encapsulation of the different layers. Note that layer 2 encapsulate the layer packet on both sides.



TCP/IP Model

The TCP/IP Model is a stripped down version of the OSI Model.



Transport Control Protocol (TCP)

TCP is a layer 3 protocol and is encapsulated by layer (Internet) and encapsulates the application layer. The protocol uses a three-way handshake (SYN, SYN ACK, SYN ACK). After the handshake it breaks down the data of the application layer into segments and ads its own header at the front of the fragement and sends it to layer 1 (Network Access).

The size of a TCP packet is based on the MTU (maximum transmission unit), a packet can never be bigger than the MTU so most of the time the data of the application layer will be broken up into segments.

TCP also handles flow control, how fast a host can send data to the client. This is done based on a *window* this window scales up and down depending on the how full the window is. If a host doesn't get enough ACK responses it will decrease the window size, it will increase the window size if it continiously receives ACK responses.

If the host doesn't get an ACK back it will resend the message that have not been ACKed. This can be done because eacht TCP header contains a *sequence number* so the host can see which packets have been ACKed. This sequence number is also used too reorder the packages in the right order to sent it to the application layer.

UDP

UDP is like TCP a protocol on the Internet layer, that is the only thing they have in common. UDP doesn't have knowledge of connections or does anything to make sure the package is send and received. The advantage of UDP over TCP is that is doesn't have the overhead of TCP (retransmitting packages, keeping track of connections etc.).

IP (IPv4 only)

This is the backbone of the internet, it allows hosts to connect to eachother. Routers uses IP addresses to route IP packets from network to network.

Ethernet

Ethernet is a protocol at the Data link layer of the OSI model. It actually contains two layers:

- **802.3 Media Access Layer (MAC)** The physical part of this layer.
- **802.2 Logical link Control (LLC)** The software part of this layer.

Ethernet does the following things on this layer:

- **Collision Detection (CSMA/CD)** If a collision occurs it will sets a timer and wait for x amount of miliseconds.
- **Encapsulation of the Network layer** Note that this encapsulation has a header and a trailer.
- **Ethernet addressing** A unique address for a single device on a LAN network. Switches uses MAC addresses to switch packets between divices instead of IP addresses.

An ethernet address is 48 bits long. The first 24 bits are for the **Organizationally Unique Identifier (OUI)**, the last 24 bits is unique to that specific NIC.

IP Addressing and Subnets

TODO

This chapter is not yet complete!

Introduction to Cisco Routers, Switches and IOS

TODO

This chapter is not yet complete!

Introduction to IP Routing

In the simplest terms, IP Routing is the process of moving packets from its source to its destination across internetworks. To be able to route packets, a router must know at a minimum the following:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- Be able to maintain and verify routing information

The following steps are taking place when a router routes a packet. *Please note that this is simplified!*

Step 1 Determine on same network by doing AND operation on source and destination

Step 2 if the destination is the same network use ARP-table for the MAC if not use default gateway

Step 3 if packet not the same network use default gateway

Step 4 router examines the MAC address

Step 5 if MAC address is in the routing table sends frame towards corresponding interface

Step 6 if router does not have a match look for default gateway

Step 7 if there is no default gateway present drop packet

As you would have realized by now, the essence of routing is how the router learns about the remote networks. Routing information is stored in the routing table also called the Routing Information Base (RIB). The RIB consists of routes to destination networks.

For direct connected entries the RIB looks liks this:

Route Source Identifies how the route was learned

Destination network The address of the remote network and how that network is connected

Outgoing interface Identifies the exit interface to use when forwarding packets to the destination network

For remote connected entries the RIB looks like this:

Route Source Identifies how the route was learned

Destination network The address of the remote network and how that network is connected

Administrative Distance Identifies the trustworthiness of the route source

Metric identifies the value assigne to reach the remote network. Lower values indicate preferred routes

Outgoing interface Identifies the exit interface to use when forwarding packets to the destination network

TODO

This chapter is not yet complete!

Routing Protocols

RIPv1 & RIPv2

RIP is a *distance vector* protocol, the only widely used routing protocol that uses the distance vector protocol today.

RIPv1 was defined as a *classful* protocol. Therefore it does not advertise subnet mask information and assumes the default subnest mask based on the class of the network.

When a router starts up, it will automatically add the connected networks to its routing table, denoting them with a `C`. If RIP is enabled, the router broadcasts its routing table. Neighbouring routers router with RIP enabled will receive the broadcast update and add the routes to their own routing tables. Each RIP enabled router will broadcast its routing table this way, therefore the routing table will converge accross the network.

RIP has the following characteristics:

- RIP sends out its *entire* routing table every 30 seconds.
- Has a maximum hop count limit of 15.
- Implements split horizon, route poisoning and holddown timers to prevent routing loops.
- High convergence time.

RIP uses 4 different timers:

Router update timer Interval between the routing table broadcasts.

Router invalid timer If a router does not head any updates about a route, it will consider that route as invalid.

Holddown timer When a route becomes invalid, it enters into holddown state. The route will remain in the routing table but the router will not accept any updates regaring this rout unless the metric is equal to or better than the existing metric.

Router flush timer While a route is in holddown state, the route is still in the routing table and will remain so for the duration specified by the flush timer.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco Proprietary classless routing protocol. It takes various features of *distance vecor* and *link state* protocols to overcome the disadvantages of a distance vector protocol.

EIGRP uses the following features of a *distance vector protocol*:

- Hop count limit of 100 by default (*up to 255*).
- Uses *routing-by-rumor* mechanism.
- Implements loop avoidance techniques.

From a *link state protocol* it inherits:

- Neighbour discovery and periodically checking their state.
- Only sends updates when changes occur.

TODO

This chapter is not yet complete!

Open Shortest Path First (OSPF)

OSPF is a *link state protocol*. Besides it is also an open standard protocol, which allows OSPF to be used in a multivendor network. Compared to EIGRP, OSPF is a more complex protocol. The features of OSPF are:

- Works on the concept of Areas and Autonomous systems.
- Highly scalable.
- Support VLSM/CIDR and dis-contiguos networks.
- Does not have a hop count limit.
- Works in multivender environments.
- Minimizes updates betweens neighbors.
- And many more features...

TODO

This chapter is not yet complete!

Switching and Spanning Tree Protocol

TODO

This chapter is not yet complete!

VLANs and VTP

MAC address table

The ultimate goal of a switch it to carry frames from source to destination based on the MAC. Switch maintains a MAC Address Table. When a switch reveives a frame it does one of these 4 type of casts

Known unicast the switch has an entry in its MAC Address Table so it forwards the frame towards the associated interface

Unkown Unicast the switch has no entry in its MAC Address Table and forwards a copy of the frame out of all interface, except the ingress port.

Broadcast same as unknown unicast. There isn't much difference between Unknown Unicast en Broadcasting.

Multicast the switch floods frame identically to unknown unicasts and broadcasts, unless certain multicast optimizations are configured.

VLAN

VLAN allows the network to be segmented based on factors like: function, location or department. VLAN creates a logical broadcast domain that can span multiple physical LAN segment. Some of the benefits are:

- Security
- Cost Reduction
- Better Performance
- Reduce size of broadcast domains
- Simple management
- Improved IT staff effiency

There are 5 types of VLAN:

Data VLAN Carries user-generated traffic. VLAN carrying voice or management traffic would not be a data VLAN (Data VLAN also called User VLAN)

Default VLAN Default VLAN in Cisco switches is VLAN 1. And all switch ports become part of the default VLAN after initial boot up.

Native VLAN A native VLAN is assigned to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.

Management VLAN A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default

Voice VLAN A separate VLAN is needed to support Voice over IP (VoIP). Needs: Assured bandwidth, Transmission,

VLAN's wouldnt be useful without trunks. A VLAN trunk extends VLANs across an entire network. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces. *switchport access vlan 10* assigns a VLAN to an interface port.

VLAN Routing

Without a router VLAN cannot be routed through the network regardless of the device used, the process of forwarding network traffic from one VLAN to another VLAN using routing is known as inter-VLAN routing. There are three types.

Legacy Inter-VLAN routing performed by using different physical router interfaces to different physical switch ports. Needs a cable for each VLAN. switch port must be in acces mode

Router-on-a-stick Router-on-a-stick is a type of router configuration in which a single physical interface routes traffic between multiple VLANs on a network. Makes use of subinterfaces. switch interface must be in trunk mode.

Layer 3 switching using SVIs Is out of scope for CCNA

Network Security

Security Introduction

Internet and networks are becoming more complex and mission critical. Through the recent years there has been an intergration of network infrastructures. As a matter of fact, no computer system in the world can be completely secure no matter how good the security measures are. Probably the only way to fully secure a computer is to isolate it completely, restricting all physical and virtual access to it. Such a system would not be connected to any network and would probably be stored in a secured vault somewhere with no physical access

Cisco IOS software running on Cisco routers has several built-in security tools that can be used as part of a good overall security strategy. Probably the most important security tool in Cisco IOS software are access control lists (ACL)

C Confidentiality - prevents acces to sensative information

I Integritiy - prevents unauthorized modification of data

A Availability - prevents the loss of acces to information

In a medium to large enterprise, the typical secured network is built around a recipe of a perimeter router, a firewall device, and an internal router:

Perimeter Router is the border between enterprise resources and the public network (internet)

Firewall Firewall allows sophisticated control of traffic flow.

Internal Router provides addtional security by providing a point for further traffic control

DMZ provides a buffer zone that seperates a trusted network from the untrusted network.

Vulnerabilities, Threats and Exploits:

Vulnerability - a weakness in a system or design which can be exploited by a threat

Threat - threat is an external danger to the system have a vulnerability

Exploit said to exist when computer code is actually developed to take advtanges of a vulnerability.

Type of Attacks

There are three major types of networks attacks:

- Reconnaissance Attacks
- Access Attacks
- Denial of Service

Counter measures

Physical and Administrative security measures

- Locks
- Biometric acces systems
- Security Traps
- IDS
- Safes
- Racks
- UPS
- Positive air-flow systems
- Fire Suppresion systems

Port Security

You can use port security feature to *restrict* who can acces the network by connecting to a switchport.

You can specify which MAC addresses are allowed to acces the port. f a port is configured as a secure port and the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation
There are three Secure MAC Address Types

Static Secure manually configured MAC addresses. Are stored in address table and added to the running-config

Dynamic Secure are dynmaically learned. Are stored in address table and are removed when the switch restarts

Sticky Secure can either be manually or dynamically learned. stored in the address table and added to running-config Sticky Learning must be enabled by the command *switchport port-security mac-address sticky*

Access Lists

An ACL is a series of IOS commands that control whether a router forwards or drops packets based on information when configured, ACL perform the following tasks

- Limit network traffic to increase network performance
- Provide traffic flow control
- provide a basic level of security for network acces
- provide a basic level of security for network
- filter traffic
- Screen hosts to permit or deny acces

Packet filtering works at Layer 3 and 4. The last statement of an ACL is always an implicit deny. This statement is automatically inserted at the end of each ACL even though it is not physically present. ACLs can be configured to apply to inbound traffic and outbound traffic.

Inbound ACL incoming packets are processed before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups

Outbound ACL incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL

A wildcard mask is a string of 32 binary digits used by the router to determine which bits of the address to examine for a match. Also note that an ACL mask is reversed meaning. example:

- `255.255.255.255 == 0.0.0.0`
- `255.255.255.252 == 0.0.0.3`
- `255.255.255.248 == 0.0.0.7`

Guide lines for creating ACL's:

- Use ACL in Firewalls between your internal network
- Use ACL on a router positioned between two part of your network
- Use ACL on border routers, that is, routers situated at the edges of your networks.
- Configure ACLs for each network protocol configured on the border router interfaces.
- One ACL per protocol
- One per direction
- One per interface

There are two types of Acces lists

Standard ACL Standard access lists use source IP addresses for matching packets.

Extended ACL Extended access lists use source and destination IP addresses for matching packets and optional protocol type information for finer granularity of control.

Network Address Translation (NAT)

TODO

This chapter is not yet complete!

Wide Area Networks

TODO

This chapter is not yet complete!

Virtual Private Networks (VPN)

VPN Concept

VPNs have several advantages over other WAN technologies:

Cost Internet VPN solutions can be much cheaper than alternative private WAN options.

Security Modern VPN solutions can be as secure as private WAN options.

Scalability Internet VPN solutions can be scaled quickly and cost-effectively to a large number of sites.

VPNs are used to transport data from a private network to another private network over a public network (*the internet for example*), using encryption. Therefore a VPN is a encrypted connection between private networks over a public network. VPNs provide the following services:

Confidentiality Prevents anyone in the middle from being able to read the data.

Integrity Ensures that data is not modified in any way.

Authentication Authentication to verify the device at the other end is a legitimate device.

Anti-Replay Hackers are unable to make changes to packets.

Key Concept

VPNs offer confidentiality, integrity, authentication, and anti-replay protection for user data.

A VPN is often called a *tunnel* because it is essentially a secure channel.

IPsec VPNs

TODO

This chapter is not yet complete!

SSL VPNs & Tunneling Protocols

TODO

This chapter is not yet complete!

GRE Tunnels

TODO

This chapter is not yet complete!

IPv6

IPv6 Introduction

Due to the shortcomings of IPv4, the Internet Protocol version 6 (IPv6) has been created. The main reason for migratig TCP/IP networks from IPv4 to IPv6 is the avaiable address space. While IPv4 uses a 32-bit address, IPv6 uses a 128-bit address. The change from IPv4 to IPv6 also impacts other protocols as well (*OSPFv3, EIGRPv6, etc.*).

Just like IPv4, the main objective of IPv6 is to enable devices to forward packets through multiple routers so they arrive at the correct destination. However, IPv6 contains a number of differences over IPv4:

- Larger address space;
- Auto-configuration;
- The IPv6 header is *not* similar to the IPv4 header;
- Extension headers/options;
- Authentication and privacy;
- Flow labels (*QoS*).

There are thee types of IPv6 addresses:

Unicast Unique address for each interface.

Anycast Multiple interfaces, packets are send to one (*nearest*).

Multicast Multiple interfaces, packets are send to all.

Key Concept

IPv6 broadcast addresses are special case of multicast addresses.

An IPv6 address is a 128-bit value, displayed as 8 groups of 4 hexadecimal digits. For example: `2001:0DB8:0000:0000:0006:0600:300D:527B`. Leading zeros can be left out: `2001:DB8:0:0:6:600:300D:527B`, one or more adjecent groups of 16 bit of zeros can be replaced with the `::` symbol (*once!*): `2001:DB8::6:600:300D:527B`.

IPv6 provides tow similar options for unicast addressing:

Global Unicast Similar to public IPv4 addresses. These addresses are allocated by the IANA. Each company is assigned a unique IPv6 address block called a *global routing prefix*. Global Unicast addresses make up the majority of IPv6 addresses.

Unique Local Similar to private IPv4 addresses. Can by used by when behind a IPv6 NAT and in networks that aren't connected to the internet.

IPv6 addresses can be identified by the initial bits of the address:

Address Type	*Binary Prefix*	*IPv6 Notation*
Unspecified	`0000 (128 bits)`	`::/128`
Loopback	`0001 (128 bits)`	`::1/128`
Multicast	`1111 1111`	`FF00::/8`
Link-Local Unicast	`1111 1110 10`	`FF80::/10`
Global Unicast	*everthing else*	*everthing else*

IPv6 Address Configuration

TODO

This chapter is not yet complete!

OSPF version 3

TODO

This chapter is not yet complete!

EIGRP for IPv6

TODO

This chapter is not yet complete!

IP Services

TODO

This chapter is not yet complete!

AAA

AAA or triple A stands for, *Authentication*, who is allowed to connect? *Authorisation*, what are the allowed to do? and *Accounting* what is done?

There are several ways to enable AAA on Cisco equipment. For simple environments a *local database* can be used. While providing more security than a simple password it is not scalable accross mulitple pieces of equipment. To solve the scalbility issue, *server based AAA* can be used. The Cisco course describes two different protocols, *RADIUS* and *TACACS+*. They can be enabled on specific login interfaces or all login interfaces and be used alongside eachother with prioritization. To provide failover capabilities, more than one server can be specified. In general *server based Authentication* works as follows. The user tries to login on equipment, the equipment verifies the login information with the server and the server responds with an allow or deny message. The communication between equipment and server makes use of an encrption key. There are serveral differences between the protocols, chosing a protocol depends on the situation.

- TACACS+
  - Seperates authentication and authorisation.
  - Encrypts all communication.
  - Uses TCP.
- RADIUS
  - Authentication and authorisation as one process.
  - Only the password gets encrypted.
  - Uses UDP.
  - Provides support for remote acces technologies, 802.1x and session innitiation protocol(SIP).

Port based authentication is another subject touched on by AAA. It makes use of the 802.1x protocol and is used to restrict workstations. Workstations that are connected to a switchport with 802.1x need to set up an authorized connection to the switch. This is done by sending out an *EAPOL-start* message to the switch. The switch verifies the workstation with the RADIUS server. Once verified, the workstation has an authorized conneciton and normal traffic can be transmitted on the connection. To stop an authorized connection an *EAPOL-logoff* message is send out. Without the authorized connection only *EAPOL* messages can be send on the connection.

---

https://github.com/roaldnefs/ccna