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

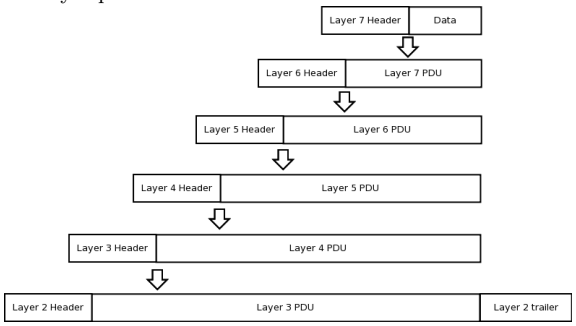
There are two important types of networks: **Local Area Network (LAN)** and **Wide Area Network (WAN)**. LANs are smaller networks most of the time, you'll find them in your home, at work, and at school. They cover a small area like a floor or a building. They can transfer a large amount of data. WANs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

OSI Reference Model

The OSI layer:

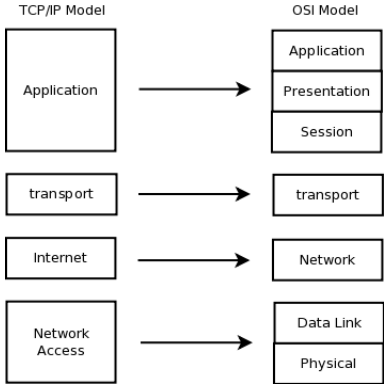
7. Application	• Provides a user interface
6. Presentation	• Presents Data • Handles encryption and decryption
5. Session	• Maintains distinction between data of separate applications • Provides dialog control between hosts
4. Transport	• Provides End-to-End connections • Provides reliable or unreliable delivery and flow control
3. Network	• Provides Logical Addressing • Provides Path determination using logical addressing
2. Data Link	• Provides media access and physical addressing
1. Physical	• Converts digital data so that it can be sent over the physical medium • Moves data between hosts

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.

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

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)

TODO

This chapter is not yet complete!

Open Shortest Path First (OSPF)

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,

TODO

This chapter is not yet complete!

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

Physicial 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

TODO

This chapter is not yet complete!

Network Address Translation (NAT)

TODO

This chapter is not yet complete!

Wide Area Networks

TODO

This chapter is not yet complete!

Virtual Private Networks

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!

---

https://github.com/roaldnefs/ccna