Telematica

Contents

Telematica 1
- Fechas 2
- Evaluacion 2
- Libros 2

Primer Parcial 2
- Dispositivos 2
- Representación 3
- Tipos de redes 3
- Internet 3
  - Intranets y Extranets 3
  - Conectarse 3
    - De negocio 3
- Red convergente 3
- Arquitectura de redes 4
- Tendencias 4
  - BYOD 4
  - Colaboración en linea 4
  - Computo en la nube 4
  - Linea electrica 4
  - Banda ancha inalambrica 5
- Terminos de seguridad 5
- 1.2 Componentes de la red 5
- 1.3 Topologias 5
- Configurar Switch y dispositivo final 5
- DIrecciones IP 6
- Mascara 6
- Protocolos 7
  - Codificación 7
  - Formato 7
  - Temporización 7
  - Opciones de entrega 7
  - Funciones 8
  - Capas de protocolos 8
  - Suites de protocolos 8
  - Ejemplos 8
  - Como funciona 8
- Estandares 8
  - Modelo en capas, importante 9
- Segmentación de datos 9
  - Capa 3, direccionamiento 9
- Dispositivos en la misma red 9
- Capa de enlace 10
  - Normas 10
  - Topología 10
  - Comunicación 11

Fechas

1. Parcial en Lunes 11 o Viernes 15 de Sep
2. Parcial en Lunes 23 o Viernes 27 de Oct
3. Examen final 3.1 Teorico Jueves 23 de Nov 3.2 De la UP Martes 28 de Nov, practico

Evaluacion

1. 1er parcial 20% (80 examen, 20 modulos)
2. 2do parcial 20% (80 examen, 20 modulos)
3. Final 40% (40 final, 40 up, 20 modulos)
4. Laboratorio 20%

Libros

1. Introduction to networks companion guide
2. CCNA 200-301 Official Cert Guide, Volume 1

Primer Parcial

- Redes en la actualidad
- Configuracion basica de switches u terminales
- Protocolos (tcp-ip) y modelos
- Capa fisica
- Sistemas numéricos
- Capa de enlace de datos
- Switchinh Ethernet
- Capa de red
- Resolucion de direcciones
- COnfiguracion básica de un router
- Asignacion de direcciones ipv4
- Asignacion de direcciones ipv6
- ICMP

Lo que hace el ping

- Capa de transporte

Los protocolos que permiten separar lo que enviamos por la red, como TCP y UDP. Tambien a nived de hardware como corregir información faltante

- Capa de aplicación

Diseño de aplicaciones que logre ser eficiente con la red

- Fundamentos de seguridad de la red
- Crear una red pequeña

Dispositivos

Hoy en dia usamos las redes en absolutamente todo.

- **Dispositivos finales**: Los que consumen y generan información: Ipad, laptop, impresora, etc.
- **Intermedios**: Mandan trafico entre los dispositivos finales, como Switches, routers, etc. No son el fin, solo son un medio que recibe y retransmite. LAN, WLAN, Wireless
- Los **medios** de red son, los *medios* por los cuales se envian los mensajes. Entre esos estan los alambricos e inalambricos.

Representación

Cómo se dibujan las cosas para que entre dos ingenieros se puedan compartir las redes que hay entre los dispositivos finales, intermedios y medios.

- **Topologia fisica**. El camino que toman los cables para llegar a todos los dispositivos de la red/ empresa, esto incluye los cables y dispositivos fisicos involucrados en las estructuras.
- **Topologia logica**. Lo que importa es el TCP-IP, cómo esta configurada la conexión de los dispositivos para que se puedan comunicar entre si. Cómo esta configurado el TCP-IP de la red.

Tipos de redes

Se clasifican por su finción y su tamaño.

- Desde redes pequeñas de dos computadoras hasta miles de computadoras.
- LANs y WANs. donde LAN es local y WAN es la red que interconecta redes LAN.

Internet

Internet es la interconexón entre todas las redes WAN y LAN, la conexión de todos los usuarios es el internet. Los provedores como AT&T, Telmex, etc son los dueños de ciertas partes de internet porque proveen las conecciones.

El internet esta regulado pori las siguientes organizaciones, para hacer que el internet sea usado de forma masiva y de forma estándard:

- IETF
- ICANN
- IAB

> El internet en cualquier parte del mundo funciona igual, lo que permitó el crecimiento exponencial de su uso, a diferencia de muchas otras cosas como los enchufes.

Intranets y Extranets

La extranet son servicios que dan empresas porque los demás lo necesitan. La intranet tiene un objetivo unico, sea esta una organización. Coleccion privada de LAN y WAN.

Conectarse

El ISP es el que da el servicio que permite que los usuarios se conecten a internet, en mexico el que más se usa es el ASDL.

- Cable: Internet de ancho de bandai siempre encendido como tele por cable.
- DSL: Ancho de banda alto.
- Red celular
- Stélite
- Telefono de marcación

De negocio

Es un internet privado, dedicado y arrendado. Un enlace de 100Mbts dedicados no es lo mismo que un enlace no dedicado, como el internet de los hogares, pues es un enlace entre miles de dispositivos, mientras que el dedicado es especifico para los dispositivos del que contrata.

Red convergente

Antes habia distintos cables para red, para internet, etc. Hoy en dia tenemos una sola red, que se le dice red convergente para tener distintos servicios, para voz, video y datos.

Datos:

- Si no hay red se cae todo, no funciona ni llamadas, ni tele, ni internet, nada.
- Es mas facil de instalar

Arquitectura de redes

Al diseñar una red se busca tener caracteristicas que van a moldear el diseño:

- Tolerancia de falla: El hardware necesario para poder mantener la red funcional, por ejemplo con **redundancia** de routers, cables, etc. Los routers redundantes pueden corregir fallas automaticamente, redireccionando a otros dispositivos intermedios.
- Escalabilidad: Poder hacer crecer una red en el futuro de forma rapida y facil sin afectar el rendimiento de los servicios. Esto se logra por medio de la estimación. Pensar de forma en que los switches y routers sean capaces de aumentar la carga.
- QoS, Calidad de servicio: El ancho de banda utilizado se pueda compartir de forma que los servicios clave no tengan que esperar por la red. Se hace un diseño de forma que a pesar de que la red este saturada, se reserve los recursos necesarios para los servicios primarios, Se hace un diseño de forma que a pesar de que la red este saturada, se reserve los recursos necesarios para los servicios primarios, es decir el QoS, similar al metrobus. En las redes se utiliza el 100% de la red para todos, excepto cuando llegan paquetes QoS, ahi se le da prioridad a los paquetes importantes, que no nos convienen que fallen nunca. Es un bit que se marca en las banderas y los dispositivos que implementan el QoS lo van a respetar. El hardware es el que marca el parquete como QoS, no los usuarios, lo hace el sistema operativo. (Aunque podre cargar modulos para marcarlos ?)
- Seguridad: Tenemos que colocar hardware que permita:
  - Confidencialidad
  - Integridad
  - Disponibilidad

  Los ataques mas fuertes comienzan en las redes.

Tendencias

BYOD

En el area de tecnologia la mayoria de empresas te dan un celular y una computadora. Las redes deben funcionar pensando en que los dispositivos que se estan usando no se usan solo para la red en la que se esta usando.

Colaboración en linea

Computo en la nube

Si mi internet es lento, al servidor que contratamos solo podemos acceder de forma lenta, por lo que en este tipo de escenarios lo que se busca es maximizar el accesso a los servicios que se rentan.

- Publica: Servicios que cualquiera puede contratar, en el mismo hardware hay muchos servicios de muchos usuarios.
- Privada: Por ejemplo un banco, contrara un servicio en la nube donde el 100% del hardware es para un solo usuario.
- Hibridas: Contratar nubes privadas en cierta cantidad, y cuando la demanda es muy alta te pido por favor que el resto de recursos necesarios para esacalar sean de recursos de nube publica.
- Personalizada: Por caracteristicas legales es neceario tener caracteristicas necesarias.

Linea electrica

Servicio que permite distribuir por medio de los cables de electricidad. PowerLine, hace de red -> energia -> adaptador -> red.

Banda ancha inalambrica
Hay ciudades donde se da servicio de forma inalambrica.

Terminos de seguridad

Existen amenazas internas y externas, los hackers buscan tener un beneficio, sea de estatus o monetario.

Obvio es mas facil atacar desde dentro de la red a lograrlo desde fuera. En el caso de estar dentro de la red se busca acceder a privilegios que no se supone que se deberian tener.

Los externos son mas frecuentes pero suelen ser de menor impacto. Hay distintos softwares que se pueden usar para bloquear y proteger como antivirus y firewalls.

- Firewalls:
  - Hardware: Mejor, mas caro
  - Software: Aplicaciones del sistema operativo y externas que dan proteccion
- Listas de control de accesso (ACL): Podemos poner en el router las restricciones que bloquean los sitios especificados.
- Prevencion de intrusiones: Se monitorea a los usuarios para detectar patrones anómalos.
- Redes privadas virtuales (VPN)

1.2 Componentes de la red

Un **host** es un dispositivo con un número especifico (IP) asignado para facilitar la comunicación, puede ser a la vez un cliente, también se les llama dispositivos finales.

Un **cliente** tiene el software necesario para solicitar y mostrar información solicitada a un servidor.

A las redes que cuentan con computadoras que funcionan como cliente y como servidor a la vez se les conoce como **redes entre pares**.

Se le conoce como **terminal** a los dispositivos a los extremos de la comunicación, es decir el emisor y receptor.

Los dispositivos intermedios conectan los dispositivos finales, proporcionan conectividad y garantizan el flujo de datos en toda la red.

1.3 Topologias

Un diagrama proporciona una manera fácil de comprender cómo se conectan los dispositivos en una red grande.

Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación del cable, como se muestra en la figura. Puede ver que las habitaciones en las que se encuentran estos dispositivos están etiquetadas en esta topología física.

Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red, como se muestra en la figura. Puede ver qué dispositivos finales están conectados a qué dispositivos intermediarios y qué medios se están utilizando.

Configurar Switch y dispositivo final

Se puede hacer que se muestren mensajes especificos a los usuarios que llegan a el prompt lo reciban

```
configure terminal
banner motd #el mensaje del dia#
```

- `startup-config`

Es un archivo con todas las modificaciones que hemos hecho en la memoria `NVRAM`, que es no volatil.

- `running-config`

  Es un archivo en la RAM, que tiene las configuraciones hechas en la sesió, si queremos hacer los cambios permantentes debemos copiar la configuración a la `NVRAM`.

  ```
  copy running-config startup config
  ```

  > Podemos mostrar los valores de configuración de cualquiera de los archivos con `show running-config`

DIrecciones IP

La máscaras se usa para saber el tamaño de la red, mientras más 0s más grande es la red.

El gateway es la IP del dispositivo de capa-3, como un router, que le da la conectividad. El *gateway* es la dirección IP de un dispositivo que le da conevtividad a los demás dispositivos, todos los dispositivos deben tener configurado el gateway, en el caso del switch, actua como una computadora más.

Todos los dispositivos pueden ser condigurados para tener una dirección IPv4 e IPv6.

hacer las 3 practicas y mandar las 8 capturas

Mascara

Podemos representar la mascara de la forma decimal o de prefijo, es decir `255.0.0.0` o `32/8`, que lo mismo y quiere decir que son 8 bits sobre los 32 que se usan de mascara. Siempre son 1s seguidos y despues son solo 0s, no puede darse `1011_1111.0000_0000.0000_0000.0000_0000`

Cuando en la IPv6 se selecciona que el prefijo de la subnet son, por poner un ejemplo, 64, quiere decir que los primeros 64 bits son con valor `1`.

Para calcular el tamaño de la red podemos usar la máscara:

$$2^{\text{numero de 0s en la ip}} - 2$$

Por ejemplo con la máscara `255.255.0.0` tenemos `16` bits que son 0, es decir $2^{16} - 2$ Otro ejemplo `255.255.255.0` o `/24` son 254 dispositivos.

Un router puede dar gateways a distintas computadoras, la importante para conocer el gateway es al que está conectado la PC.

El `::` significa todo lo que falte por conocer, en este caso significa porner todo lo que haga falta para ser 0s que cumplan con el número de hextetos, o sea 8?

En la IPv4 se usan 4 octetos de 8 bits, en cambio en IPv6 se usan hextetos (hexadecimal), son 8 con 16 bits en cada uno.

Un solo hexteto esta separado por `:`, no confundir con `::`

Hay dos modos de configurar la red, como configurar la red a mano o hacerlo de forma DHCP.

Interfaz virtual: tenemos distintas capas

- Capa 1: Hardware
- Capa 2: Sowftware + Hardware, aqui hay switches, se usa la dirección MAC No hay ningun tipo de configuración sobre IP, hay una interfaz logica del switch, que no es de hardware pero permite adminsitrarlo remoto

```
configure terminal
interface vlan 1
ip address <ip> <mascara>
no shutdown
```

Con eso logramos poenr una IP a la vlan 1, que es una puerta virtual del switch, con la que va a responder, un ejemplo, a alguien no le da red, hacemos ping a todos los switches y vemos cual está apagado

- Capa 3:

Protocolos

Los protocolos dan:

- Emisor y receptor
- Idioma y gramatica comun
- Valocidad y momento de entrega
- Requisitos de confirmación o acuse de recibido (ACK)

Requisitos de los protocolos:

- Codificar los mensajes, pasar de mensaje a binario, o a nubes, etc
- Formatear y encapsular el mensaje
- Tamaño del mensaje
- Sincronización del mensaje
- Opciones de entrega del mensaje

Codificación

Al mensaje lo codificamos, lo enviamos por el medio y el receptor decodifica el mensaje y lo interpreta, esto implica que el receptor debe tener el mismo conocimiento que nosotros en el formato del mensaje y cómo lo codificamos.

Formato

Suele existir un encabezado con *metadata* sobre a quién va, que versión, y demás información, despues se envia el mensaje(s).

El tamaño del mensaje se limita por el tamaño de la red, dependiendo del medio se usan mensajes de tamaño distintos, en el rango de 64 bytes a 1500 bytes, es por esto que después se dividen los paquetes en múltiples. Si un paquete es menor de 64 o mayor a 1500 se considerará como corrupto el mensaje.

Temporización

Control de flujo, administrar la estrategia usada para enviar/recibir paquetes Tiempo de espera: El timeout si no recibe más paquetes. El método de accseo: Permite que los paquetes colisionen lo menos posible.

Opciones de entrega

- Unicast: Se transmite a un solo dispositivo
- Multicast: Se transmite a uno o varios
- Broadcast: Se transmite a todos

Esto en realidad pasa que se envia el paquete a todas las máquinas, las que no son las receptoras tiran el paquete, lo ignoran, la o las máquinas que si son receptoras lo procesan.

En la seguridad puede que para cuando logremos descifrar la persona ya haya cambiado la contraseña o la situación de la información, es decir que la información perdió valor.

Funciones

Los protocolos de red funcionan de forma aceptable. Los protocolos son un poco anárquicos, hacen su mejor esfuerzo, lo intentan enviar lo mejor que pueden, mas no se puede garantizar que funcione.

Pone por ejemplo una aduana, no se revisa a todas las persona, se reviza solo a algunas personas para apaciguar a posibles personas que piensen en hacer algo malo. Otro ejemplo es medio revisar a todos, muy por encima, y reducir el numero de verificaciones que deben ser hechas con precision al minimo.

Capas de protocolos

Los protocolos interactuan, hay 4 capas

- HTTP:
- TCP/QDP : Que tipo de paquete tengo, si veracidad o velocidad
- IP:
- Ethernet:

Suites de protocolos

Se clasifica en:

- Es el Medio, transport layer
- Usa Contenido,
- No se que

Cada empresa solia tener sus propios suites de protocolos, el conjunto de ellos lograba la conexión, comunicación y procesamiento de los paquetes. Hoy en dia está estandarizado el TCP/IP.

Ejemplos

1. Network
- ARP: Para identificar con MAC e IP
- Ethernet: para conexión fisica
- WLAN: Lo mismo wireless
2. Internet
- NAT: Convierte IP privada a publica
- IPv4, IPv6
- Routing Protocols: Estrategia de ruteo
3.
- TCP
- UDP
4. Aplicación
- DNS: Resolución de dominios
- DHCPC: Asignación dinámica de IP
- De correos

Como funciona

Cualquier dato que se quiera enviar lo encapsulamos, le ponemos un encabezado TCP/IP, le decimos IP de destino en otro encabezado y agregamos un encabezado que se le llama Frame. Todo eso como binario se manda al cliente, que desencapzula, interpreta, procesa, etc.

Estandares

IEEE: La de ingenieros IANA: Direccionamiento IP, se encarga de administrar los dominios y su direccionamiento a la IP IETF: Hardware Intenet Society: Investigación especifica del internet

- Normativas, investigacion

•

Por ejemplo, hacer que cualquier norma inalambrica nueva, sea totalmente retrocompatible con elementos de hace 25 años.

Modelo en capas, importante
Es la norma ISO del modelo OSI, se usa a nivel mundial para todo tipo de comunicaciones
- Basada en 7 capas:
  1. Fisica, Physicial: Hardware
  2. Enlace de datos, Data link: Aqui rescide el frame, atiende fisico y soft
  3. Redes, Network: Red, IPs, etc
  4. Transporte
  5. Sesión, Session: Sesión entre aplicaciones, como se comunican entre si aplicaciones
  6. Presentacion: Formato, como mp4, bin, etc
  7. Aplicación: Aplicaciones que procesan los datos
  8. Persona, la ignoracia del usuario: Por ejemplo, no esta conectada la computadora.

El modelo ISO/OSI en la red es la TCP/IP
1. Acceso de red, Network Access, 1 y 2
2. Internet, 3
3. Transporte, 4
4. Aplicación

Los dos modelos están muy relacionados. Los beneficios de trabajar en un modelo por capas es que puedes concentrarte/especializarte en la capa de tu interés sin tener en cuenta cómo están funcionando capas por debajo y por arriba de tu área de especialización.

Segmentación de datos
Dividir y conquistar, ayuda a aumentar la velocidad, despeja el tiempo que se usa un camino de comunicación por un solo paquete, aumenta la eficiencia. Igualito que Unix, donde vamos segmentando el recibir un paquete en multiples fracciones.

Esto implica que los paquetes tienen forma de identificar la secuencia de los mismos. Para lograrlo hay una estructura de datos que se debe respetar:

- Data 64-1500 bytes
- Segmento: Si es TCP/UDO
- Paquete:
- Frame
- A bits

Los paquetes llevan un checksum para verificar que el paquete está integro, llevan bits como mecanismos de seguridad. Usar algun tipo de verificación es necesario, aun cuando sean mecanismos sencillos pueden ayudar a reducir la probabilidad de error.

Capa 3, direccionamiento
Se arma un paquete con direccion de origen y destino, pueden ser IPv4 o IPv6, aunque tenga dos direcciones al final va a mandar los paquetes en un tipo de red.

Dispositivos en la misma red
Podemos identificar distinas sub-redes viendo los cables que salen de un solo router. Cuando un dispositivo quiere mandar paquetes a computadoras en su misma red se hace de forma directa, si no

está en su rango se lo envía a su *gateaway*, el *gateaway* (router) se encarga de enviar el paquete a donde debe ser para que lo reciba la máquina en la otra red, lo *enruta*.

Cuando el paquete va viajando en el tramo Origen a destino tienen la IP de destino final, más la IP de la maquina a la que va esta incluida, que es la MAC, asi las computadoras en realidad se comunican por MAC.

Entonces aunque diga que tiene una ip para otra maquina fuera de la red, entonces se incluye la IP peeero la dirección MAC de destino será el Gateaway, cada salto entre routers hay cambio de dirección MAC, mas la IP final es la misma.

Los routers deciden por donde se va a enviar el paquete, solo deciden a cuál de los routers simplemente deciden a qué siguiente router enviarlo, más no fijan toda la ruta, cada router hace su propio calculo para enviar el paquete segun su información. Los routers solo deciden el *next hub*. Siempre se termina tomando la mejor decision.

> Las redes se congestionan rapido, cuando una red se congestiona, los paquetes se van acumulados y van al router de la universidad, que despues van al internet. Mientras vamos llegando hasta arriba de la cadena de la red que sale a internet ponemos switches especiales que permiten servir de router que optimiza.
>
> Un switch sirve como balanceador de carga

> Nota, los switches son de capa 2, no pueden ser gateaways, a menos que se un switch especial que puede ser gateaway

Capa de enlace

Comunicación entre tarjetas de intrerfaz de red

La capa 2 es la que atiende las tramas. Es la única que depende de la capa física.

Normas

- Ethernet
- WLAN
- PAM (p. ej. Bluetooth)

Logrado por:

- IEEE
- ANSI
- ISO
- ITU

En esta capa se hace referencia al siguiente segmento de la red.

Topología

- Fisica: Cableado, donde estan fisicamente las cosas, etc
- Logica: Hace referencia solo a los dispositivos y sus interfaces, como sus conecciones

Topologia WAN:

- Punto a punto: Origen destino
- Hub and spoke: Uno a varios
- Malla: Todos con todos, o casi todos. En todos con todos es *full mesh* o malla completa. Tipicamente es un router y N AP, el profe tiene 3 routers

Topologia LAN (interna):

- Estrella
- Estrella expandida: Varias estrellas conectadas con switches
- Anillo: Se suele usar con la fibra optica
- Bus: Usa un cable negro obscuro.

Comunicación

- Sem-duplex: Se puede mandar o recibir, más no ambos, se usa un medio compartido
- Full duplex: Hay un medio para mandar y otro para recibir