Repubblica Italiana
Provincia Autonoma di Bolzano - Alto Adige
Republik Italien
Autonome Provinz Bozen - Südtirol
Istituto d'Istruzione Secondaria Superiore per le scienze, le tecnologie e i servizi
"GALILEO GALILEI"
Oberschulzentrum für Wissenschaften, Technologie und Dienstleistungen
ISTITUTO TECNICO TECNOLOGICO - LICEO SCIENTIFICO-SCIENZE APPLICATE
ISTITUTO PROFESSIONALE PER L'INDUSTRIA E L'ARTIGIANATO - ISTITUTO PROFESSIONALE ODONTOTECNICO
Fachoberschule für den Technologischen Bereich - Realgymnasium mit Schwerpunkt angewandte Naturwissenschaften
Berufsbildende Oberschule für Industrie und Handel - Berufsbildende Oberschule für Zahntechniker
39100 BOLZANO- via Cadorna 14
Cod. Fisc. 80006520219
39100 Bozen - Cadornastraße 14
St.Nr. 80006520219

PROF. *ALFREDO CANTARELLA*

CLASSE: *5°F* ***anno scolastico:*** *2018/19*

PROGRAMMA (effettivamente svolto) di: *"SISTEMI E RETI"*

Argomenti: *(parte teorica)*

- Definizione esatta di domini broadcast e di domini di collisione: significato, analogie e differenze, problematica di dimensionamento dei broadcast domain (BD) L2 e L3 e relative relazioni di inclusione per ottimizzare la bandwith, caratterizzazione dei collision domain (CD) mediante hub e switch, segmentazione ottimale della rete/microsegmentazione, separazione dei BD e dei CD ad opera di router e switch.

- Introduzione alle VLAN: definizione formale e relazione con in broadcast domain, vantaggi dell'uso delle VLAN in associazione alle reti IP nella definizione delle reti/gruppi logici. Metodi di creazione delle vlan, ossia di assegnamento degli elementi ad una vlan: transparent assignment tramite mac-address ed ip address, port-based, cooperative e per-user assignment tramite IEEE 802.1x, vantaggi/svantaggi e relative analogie.
- Vlan basate sulle porte switch: definizione esatta di porte switch e link in access mode e trunk mode e relativo significato, esempi specifici di applicazione/contesti d'uso. Regola fondamentale di comunicazione tra le vlan: Vlan isolation e relative implicazioni/corollari per i frame e domini broadcast L2.
- Uso e significato della VLAN 1 come vlan di default e relative proprietà fondamentali, differenza di utilizzo delle porte degli switch in ambito vlan e non, esempio di comunicazione tra host della stessa vlan agganciati a porte dello stesso switch e di switch diversi, necessità d'uso del tag relativo alla vlan d'origine per il rispetto della vlan-isolation-rule.

- Caratteristiche fondamentali dei link d'accesso e trunk e differenza tra trunk fisico e logico. Elementi fondamentali del funzionamento del protocollo IEEE 802.1q per la gestione dei tag fisici e logici dei frame in ambito VLAN, analisi in dettaglio dei campi del tag fisico su frame Ethernet, VLAN nativa, traffico taggato e non taggato.
- Trattazione sistematica del funzionamento del protocollo IEEE 802.1q ed analisi dei frame nei vari casi: frame entrante o uscente su un link d'accesso, frame entrante o uscente su un trunk logico e relativa discussione in termini di vlan permesse,

creazione e rimozione di tag fisici e logici, buffer di input ed output degli switch, frame taggati o non taggati.

- Classificazione delle VLAN in base allo scope/ambito d'uso: vlan di default, nativa, dati, d'amministrazione e voice; caratteristiche fondamentali di ciascuna categoria ed analisi dei link tra uno switch di rete, un telefono IP(Voip) ed un end-device per la vlan voice. Normal ed extented range per le VLAN: analisi e confronto delle proprietà fondamentali.
- Relazioni tra VLAN(port based assignment) e reti IP: vlan diverse all'interna della stessa rete ip e relative problematiche/vantaggi in termini di sicurezza, stessa vlan presente in reti ip diverse e relativo significato, esempi specifici per ogni caso. Regola di ottimizzazione delle VLAN: superamento della regola di vlan isolation degli switch attraverso i router ed impostazione delle regole di firewalling sulle vlan
- tramite corrispondenza esatta tra vlan (BD l2) e reti ip (BD l3).

- Intervlan routing tra vlan diverse: uso della regola di ottimizzazione delle vlan e router on access-link mediante link d'accesso/NIC distinti/separati associati alle singole vlan/reti ip tra lo switch core ed il default gateway/router corrispondente, analisi del numero di NIC fisiche necessarie per il routing e relativi svantaggi.
- Intervlan routing tra vlan diverse: uso della regola di ottimizzazione delle vlan e router on a stick (router one arm/router on a trunk) con divisione, tramite virtualizzazione gestita dall'O.S., della NIC fisica in diverse sub-interface logiche/virtuali associate alle singole vlan/reti ip tra lo switch core ed il default gateway/router corrispondente e relativi vantaggi/svantaggi.
- Intervlan routing tra vlan diverse: uso della regola di ottimizzazione delle vlan e router on SVI/interface vlan associate alle singole vlan/reti ip mediante switch core L3/multilayer fisici o logici usati come default gateway/router corrispondente e relativi vantaggi/svantaggi. Proprietà e differenze tra switch L3 (fisici e logici) e switch L2 in relazione alle SVI.

- Analisi del funzionamento del routing tramite router on SVI su switch L3: comportamento assunto in caso di frame con mac-address destinazione appartenenti a quelli d uno switch o di una SVI, determinazione in due step tramite routing table e mac-address-table della porta switch fisica usata nel caso in cui l'outgoing interface nella routing-table è una vlan-interface.
- Analisi sistematica dei vari modi possibili di collegamento tra un router ed uno switch: uso di access e trunk link, routed port e SVI su tramite switch L3.
- Analogie/differenze tra subinterface e SVI in termini di associazione ad interfacce fisiche, mac-address usati e prestazioni fornite per il forwarding di pacchetti ip.

- Introduzione al firewalling e caratteristiche fondamentali dei firewall: impostazione dei filtri/policy di sicurezza per la regolazione del traffico in entrata ed uscita verso/da una LAN, firewall HW e SW, integrati in router (router con FFS) ed indipendenti, SPF firewall, proxy firewall e differenze con i proxy-server. Definizione, uso e significato delle ACL per la configurazione delle policy su firewall.
- Uso, classificazione ed analisi delle ACL per la configurazione di SPF firewall ai livelli network(3) e transport(4): parametri d'uso delle ACL (indirizzi IP di host/reti IP, protocolli usati ai livelli 3 e 4, numeri di porta logica) a livello sorgente e/o destinazione, ACL standard ed estese, numbered e named, per IPv4 e IPv6. Ambiti d'uso delle ACL standard ed estese e relativa regola di applicazione ottimale rispetto alla posizione degli host sorgenti e destinazione.
- Regola di applicazione ottimale delle ACL standard ed estese rispetto alla posizione degli host/reti sorgenti e destinazione: analisi e motivazioni della scelta migliore e considerazioni in merito a qualunque altra scelta non ottimale in termini di traffico potenzialmente permesso(permit) e negato(deny). Applicazione delle ACL in entrata (inbound ACL) e/o in uscita (outbound ACL) su un'interfaccia L3: analisi delle differenze e relazioni con la routing-table.

- Esercitazione sull'applicazione delle ACL standard ed estese in modalità INBOUND e OUTBOUND, sui router/firewall presenti in un sistema di reti, secondo la regola di applicazione ottimale in base alla posizione tra host sorgenti e destinazione.

- Uso e significato degli operatori bit a bit or, and e xor, determinazione dell'indirizzo IP di rete di appartenenza di un host destinazione attraverso l'and bit a bit tra l'ip-address dell'host e la propria net-mask, (ai fini del rispetto delle regole fondamentali di routing). Analisi della rete madre 0.0.0.0/0 e delle motivazioni per cui viene usata come default-static-route nelle tabelle routing (matching universale con ogni ip-address).

- Uso, sintassi ed analisi delle ACL estese ed analogie con quelle standard, esempi di applicazione delle ACL estese per il filtraggio di traffico (in entrata/uscita da una LAN) L3/L4/L5 tra sorgente e destinazione usando protocolli L3/L4 ed i numeri di porta logica per i servizi sulla rete.

- Introduzione alla security in ambito VLAN e relative regole fondamentali da seguire per una buona progettazione: uso/non uso della vlan di default, messa in shutdown ed in access-mode delle porte switch non usate, uso della vlan black-hole, della stessa native-vlan in entrambi i lati di trunk-link, della native-vlan mai usata/definita per gli

host, separazione del traffico user/dati, di amministrazione e voce su vlan diverse ai fini della sicurezza e dell'ottimizzazione della bandwith.

- Analisi e risoluzione dei tipici problemi di vlan-hopping: vlan leaking/native vlan mismatch, switch spoofing e conseguente sniffing sulla rete, double tagging/double encapsulating.

- Introduzione alla route/prefix-summarization/aggregation in ambito ISP: ambiti d'uso, summarization statica e dinamica attraverso i dynamic routing protocol, motivazioni d'uso ai fini dell'ottimizzazione delle dimensioni delle routing-table e del relativo procedimento di lookup degli ip-address per il routing dei pacchetti IP. Algoritmo di summarization per la determinazione della rete IP madre ottimale a partire da un insieme di sottoreti IP.
- Condizioni necessarie per l'applicazione della route/prefix-summarization/aggregation in ambito ISP: contiguità delle reti IP, con relativo significato/definizione su IPv4 ed IPv6, e raggiungibilità attraverso la stessa outgoing interface o lo stesso next-hop. Uso, definizione e significato di supernet e supernetting/CIDR e relative applicazioni.

- Uso, analisi, ambiti d'uso di indirizzi IPv4 speciali/notevoli e relativa proprietà di ip-address routable con eventuale configurazione su NIC: 0.0.0.0 (come valore non definito), local e directed broadcast, loopback ip-address (127.x.y.z/8) e relativo significato in termini di stack ISO/OSI o TCP/IP, configurazione su NIC ed uso per server test come indirizzi virtuali, esempio di localhost come 127.0.0.1.
- Uso e significato degli indirizzi IPv4 speciali/notevoli multicast: link-local, link-global ed administrative-multicast, definizione dei relativi range di valori e contesti d'uso: dynamic routing protocol, giochi on line, video e audio broadcast, SW distribution, news feed, test di amministrazione; esempi specifici con i routing protocol ed NTP (224.0.1.1). Indirizzi IPv4 sperimentali (RFC 3330): range dei valori usati, ambiti d'uso e proprietà di non configurabilità sulle NIC.

- Indirizzi IPV4 speciali/notevoli: Introduzione agli indirizzi IPv4 privati (RFC 1918) e pubblici (classless), definizione e range dei relativi valori, significato in termini di indirizzi relativi/replicabili ed assoluti/unici in ambito LAN e/o WAN, motivazioni storiche legate all'esaurimento dello spazio d'indirizzamento IPv4, assegnazione da parte degli ISP e traslazione degli indirizzi IPv4 privati/pubblici nel passaggio LAN-WAN tramite tecnologia NAT (RFC 1918) ad opera di router/firewall.
- Caratteristiche generali della tecnologia NAT: traslazione, secondo le specifiche dell'ISP, in uscita (LAN --> WAN pubblica=Internet) degli ip-address sorgenti privati in ip-address pubblici e traslazione in entrata (WAN pubblica=Internet --> LAN)

degli ip-address destinazione pubblici in ip-address privati, relazioni tra NAT e spazio d'indirizzamento IPv4 nelle reti attuali; esempi di traslazione nel passaggio LAN --> WAN e viceversa tra client e server.

- Indirizzi IPV4 speciali/notevoli: Introduzione agli indirizzi IPv4 shared (RFC 6598) usati in ambito WAN dagli ISP, definizione, proprietà, range dei relativi valori ed analogie con i corrispondenti indirizzi IPv4 privati. Uso degli indirizzi IPv4 speciali link-local e test-net, ambiti d'uso e proprietà fondamentali di routing da configurare esplicitamente sui router per un corretto utilizzo.

- Stub-network e stub-router: definizione, analisi e proprietà fondamentali: uso di un solo router attivo con una sola interfaccia attiva per il collegamento LAN-WAN, uso di eventuali altri router e/o interfacce di backup, uso della dafault-static-route nel tratto LAN-- >WAN e delle route statiche standard/esplicite nel tratto inverso WAN--->LAN, disabilitazione dei dynamic-routing-protocol nel link LAN--WAN e relative motivazioni. Esempi di LAN SOHO come stub-network.

- Uso, analisi e significato dei parametri metrica (M) e distanza amministrativa (AD) di una route all'interno della routing table ed introduzione alle floating static route/backup route: importanza, ambiti d'uso e relativa configurazione attraverso la AD.
- Uso, e configurazione del load-balancing nel routing dei pacchetti IP effettuato da un router/switch L3: significato, impostazione del numero massimo di route su cui bilanciare il traffico, analisi e problematiche del load-balancing su TCP e UDP.

- Introduzione al dynamic addressing information: significato ed ambiti d'uso, (utenti mobili, client e server con restrizioni), protocolli/metodi stateless e stateful usati su IPv4 (stateful DHCPv4) e IPv6 (stateless SLAAC, stateful e stateless DHCPv6) e relativo significato e principi di funzionamento, elementi necessari per il funzionamento del DHCP, attivazione automatica dei client DHCP (boot ed aggancio cavo di rete su NIC) e scenari possibili iniziali (address/lease origination e renewal), modalità di assegnazione degli indirizzi IP da parte dei server DHCP (manuale, dinamica, automatica) e relative analogie/differenze.
- Addressing information fornite in modalità dinamica (con stateful DHCPv4, stateless SLAAC e stateless/stateful DHCPv6): ip address e netmask, default-gateway e DNS ip address, parametri vari, informazioni/parametri opzionali ed obbligatori in fase di configurazione e nella pratica.

- Analisi in dettaglio e sequenziale delle quattro fasi (four way handshake) di una

transazione tra client e server DHCPv4 (DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK/DHCPNACK) e relative analogie/differenze, pacchetti trasmessi in local broadcast ed unicast e relative motivazioni, analisi degli indirizzi L2, L3, L4 (porte UDP well known di client e server), valori usati per i campi fondamentali dei pacchetti DHCP durante la transazione e relativo significato (type/op-code, hardware-type, transaction ID, CHADDR, CIADDRR, YIADDR, SIADDR, SNAME, GIADDR, DHCP-OPTIONS), uso e significato del relay-agent per l'inoltro dei local broadcast usando certi protocolli di livello application basati su UDP, uso delle entry fittizie nella cache-ARP del server e del relay-agent, uso del "ping" e dell'ARP-request per la conferma del dynamic ip address da parte di server e client rispettivamente.

- Analisi in dettaglio e sequenziale delle due fasi (two way handshake) di una transazione tra client e server DHCPv4 nello scenario iniziale di address/lease renewal (DHCPREQUEST, DHCPACK/DHCPNACK), pacchetti trasmessi in local broadcast ed unicast e relative motivazioni, trasformazione del two-way-hanshake in four- way-handshake in caso di non raggiungibilità del server DHCP e relative analogie/differenze rispetto allo scenario di address/lease origination. -

- Introduzione agli attacchi di tipo MiM (man in middle) e DoS, mac-address flooding/mac-address table overflow, "DHCP-Starvation" e "DHCP spoofing", ai principi e meccanismi di attacco, alle problematiche di rete che si vengono a creare e possibili soluzioni.
- Analisi e discussione sulle generalità degli attacchi man-in-the-middle, DoS e DDoS, a forza bruta, ai principi e meccanismi di attacco, alle problematiche di rete che si vengono a creare e possibili soluzioni.
- Analisi e discussione sull'attacco mac-address -flooding su uno switch, ai principi e meccanismi di attacco, alle problematiche di rete che si vengono a creare e possibili soluzioni: uso del port-security e del protocollo IEEE 802.1x per il blocco delle porte swich in caso di accesso non autorizzato.

- Analisi in dettaglio dei possibili attacchi ad un server DHCP e delle possibili soluzioni: dhcp-starvation attack, dhcp-snooping attack e relative modalità d'uso e finalità d'esecuzione, uso del port-security e del dhcp-snooping sugli switch di rete come meccanismi di difesa mediante configurazione delle porte switch in modalità untrusted(blocked) e trusted(unblocked), filtrando il traffico delle transazioni DHCP tra client e server.

- Analisi sistematica in dettaglio del NAT-process: NAT-router e relazioni con border/edge-router e non , ip-masquerade come conseguenza del nat-process,

aggiunta di uno o più gradi di privacy e security mediante applicazione multipla del nat-process su uno o più router, uso e struttura della NAT-table, NAT-pool ed indirizzi ip pubblici e privati usati nel local loop/last mile, inside ed outside network, uso e significato degli indirizzi IPv4 inside-local, inside-global, outside-local, outside-global e relativo processo di traslazione tra inside ed outside network mediante NAT-table e configurazione delle interfacce inside ed outside in un NAT-router.

- Analisi delle varie tipologie di NAT e relativi ambiti d'uso/applicazioni: SNAT (static NAT), DNAT (dynamic NAT), PAT (port address traslation) e port forwarding (tunnelling, reverse PAT, virtual server) come casi specifici di DNAT ed SNAT con overload/overloading, associazioni statiche o dinamiche nella NAT-table tra gli inside-local-address e gli inside-global-address con cardinalità (n:m), (n:1), (1:1) nelle varie tipologie e relative logiche di associazione (one-to-one, FCFS) e timeout di traslazione, uso del numero di porta logica in associazione all'ip-address nei casi di PAT e port-forwarding, vantaggi e svantaggi per ognuna delle tipologie di applicazione NAT.
- Uso e configurazione del NAT-process nelle varie tipologie (SNAT, DNAT, PAT, port-forwarding) e step logici fondamentali da seguire: creazione dei NAT-pool, degli insiemi di host traslabili/nattabili /NAT-host), binding/mapping tra i NAT-host ed i NAT-pool, uso dell'ip-address su un'interfaccia wan/outside del nat-router, configurazione del nat, nelle varie forme, su router Cisco.

- NAT in overlapping (OAT), significato e relativi esempi, traslazione statica dell'outside-local (destinazione) in outside global in entrata su un'interfaccia inside, traslazione statica dell'outside-global (sorgente) in outside local in entrata su un'interfaccia outside.
- Analisi e discussione dei principali vantaggi e svantaggi dell'applicazione del NAT-process: conservazione dello spazio d'indirizzamento IPv4, IP-masquerade e conseguente aumento del grado di privacy e security su una LAN per ogni nat-process attivo, decremento delle prestazioni del routing per l'analisi e la modifica dei pacchetti IP e dei segmenti TCP/UDP e conseguente riscrittura delle checksum, perdita della tracciabilità nella comunicazioni end-to-end, maggiore complessità nell' applicazione dei protocolli di tunnelling per le VPN. Ordine d'applicazione del NAT-process in caso di applicazione di ACL inbound ed outbound sulle interfacce del nat-router rispetto a quello della routing-table.

- Inizio trattazione, discussione e svolgimento delle tracce delle seconde prove scritte di "Informatica e Sistemi e Reti" all'esame di stato: indicazioni generali e suggerimenti da seguire per ottenere una buona soluzione.

- Proprietà dei cavi Ethernet in rame(CAT5, CAT5e, CAT6, CAT6a, CAT7) in termini di bandwidth, frequenza di trasmissione del segnale e distanza massima coperta. Cablaggio IEEE (in fibra ottica/OC) 1000BASE-LX e 1000BASE-ZX per Ethernet WAN e distanze coperte.
- Analisi, trattazione e discussione delle possibili soluzioni della prima e seconda simulazione della 2° prova scritta per l'esame di stato (Informatica e Sistemi e Reti).

- Confine tra rete LAN e WAN, punto di demarcazione, local loop: uso e significato di DTE, DCE, CPE, borchia, ufficio terminale/local central office/centrale telefonica/POP, wan switch/switch d'accesso alla wan, core router e multilayer switch, toll Network/WAN service provider Network; uso degli access-server per vecchie connessioni in dial-up, uso e significato di DISLAM e CMTS per connessioni in xDSL e cable-network, variante HFC e relative specifiche sui TRUNK ed i FEEDER. Local loop in FTTH, FTTB, FTTC/FTTS, FTTW/FTTR, FTTN e relative specifiche.
- Classificazione gerarchica delle connessioni alla WAN di un ISP in base ad accesso pubblico o privato e relativi protocolli L2 usati. Connessioni private: linee dedicate/punto-punto/leased ed uso dei protocolli HDLC e PPP, connessioni circuit switched ed uso delle reti PSTN ed ISDN con protocollo PPP, connessioni packet switched ed uso dei protocolli Frame Relay, ATM, Ethernet WAN/MetroEthernet/EoMPLS/VPLS, MPLS. Connessioni pubbliche in broadband: linea xDSL, cable network e protocollo PPP, connessioni wireless satellitari con protocollo VSAT, connessioni in WIMAX, WIFI municipale, connessioni in 3G/4G/5G ed uso del protocollo PPP e dei protocolli specifici UMTS, HSPA, WCDMA, LTE e WIMAX. Velocita di trasmissioni supportate e distanze coperte con ciascuna tipologia di connessione.

- Uso, proprietà ed ambiti d'uso delle linee dedicate/leased/punto-punto: disponibilità permanente della linea, banda costante, assenza/limitazione massima della latenza/ritardo di Tx e del jitter, collegamento di sedi/LAN diverse appartenenti alla stessa organizzazione attraverso una WAN privata, uso di reti IP private /30. Implementazione, a livello fisico/L1, delle linee dedicate tramite interfacce seriali T1/E1, T3/E3 e tramite OC e relative velocità di trasmissione, uso dei protocolli L1 SONET, SDH e DWDM nelle reti dei provider e delle tecniche TDM e STDM per il multiplexing di ogni canale fisico. Definizione generale di VPN ed implementazione implicita delle VPN L2 tramite linee dedicate.

- Analisi in dettaglio L2 del funzionamento dei collegamenti ad una WAN di un ISP, sul local loop, tramite linea ADSL e cable -network, uso e funzioni del DSLAM e del

CMTS per le rispettive linee/reti e relativi protocolli L2 usati (PPP, DOCSIS), analisi del bridging tra i vari protocolli L2 ad opera dei modem xDSL (ADSL, SDSL, VDSL) e dei fiber-modem su collegamenti di tipo FTTx ed uso dei protocolli Ethernet ed PPPoE in maniera corrispondente tra router e modem collegati reciprocamente.

- Classificazione delle connessioni ad una WAN in base al numero di ISP a cui ci si aggancia ed al numero di link usati con ogni ISP: homed e dual homed connection, multihomed e dual multihomed connection e relative proprietà, vantaggi e svantaggi.

- VPN, tecnologie e relativi protocolli usati: Definizione esatta, significato e contesti d'uso, VPN site-to-site e Remote-Access, (client/host-to-site e client/host-to-client/host), uso e ruoli dei VPN gateway , (concentratori VPN), client/server VPN, formazione delle VPN peer network, VPN tunnel, traffico interessante e non interessante, classificazione e ruoli dei protocolli passenger/encapsulated, tunneling/carrier/encapsulation e transport delivery, VPN create in modalità tunneling e transport, relazioni tra VPN tra NAT.
- Analogie e differenze tra PPTP/L2TP VPN(L2 VPN), IP-sec VPN (L3 VPN) e SSL/TLS VPN (application layer VPN), protocolli usati per autenticazione, integrità e segretezza/confidenzialità dei messaggi, generalità dei meccanismi usati per l'autenticazione e l'integrità dei messaggi. Struttura generale delle PDU L3 usate per le VPN in modalità tunneling e transport ed, in particolare, con VPN IPsec e VPN SSL, e relativa configurazione/funzionamento dei VPN gateway.
- Funzionamento/configurazione dei VPN client e del VPN gateway (ssl/tls, IPsec) in modalità tunneling e transport: definizione su gateway degli account, degli ip-address virtuali da associare in 1:1 con gli host remoti e degli host/reti ip di accesso per ogni ip virtuale; scrittura di ip address sorgente virtuale e destinazione remota e valore di TTL a livello applicativo (transport mode) o sul pacchetto ip interno (modalità tunneling), rigenerazione dei pacchetti ip in entrata ed uscita dal VPN gateway. Elementi generali del protocollo GREP per la creazione di VPN tunnel L3 in chiaro, GRE over IP, GRE over IPSEC e relativo significato e struttura dei PDU.

- Reti WIFI e WLAN: tecnologie e standard LAN wireless IEEE 802.11x, componenti di una rete LAN wireless, collegamenti tra AP alla rete cablata tramite switch, topologia ad HOC-mode ed infrastructure-mode, association mediante rilascio al client di una porta logica dell'AP/AID e relativa propagazione allo switch collegato, gestione dei canali in una WLAN, possibili minacce per una LAN wireless e relativi meccanismi di sicurezza. Metodi/protocolli di autenticazione WEP, WPA, WPA2/IEEE 802.11i, algoritmi per la crittografia dei dati AES e TKIP, autenticazione

WPA2 personal ed enterprise (tramite IEEE 802.1x e server RADIUS).

- Caratteristiche fondamentali dei firewall SPI con o senza porta DMZ, interfacce interne, esterne, ACL e altre security-policy per il filtraggio del traffico outgoing ed ingoing attraverso le interfacce del router/firewall (router con FFS).
- Protezione, tramite firewall SPI, dei server di una LAN dagli attacchi DoS mediante impostazione di policy di sicurezza: blocco dei ping esterni (provenienti dalla WAN) e/o interni (provenienti dalla rete interna), limitazione degli attacchi ICMP flood, UDP flood e TCP SYN flood (max n° pacchetti al secondo).
- Uso/configurazione di firewall separati/indipendenti su un sistema di reti con architettura multilevel: uso delle SVI su switch-core per le VLAN interne(area trust), implementazione della DMZ, collegamenti con lo switch core/core-distribution per la parte LAN e col router per la parte WAN, uso e configurazione delle interfacce inside ed outside del firewall e delle interfacce interne ed esterne del router, ACL applicate alle interfacce di entrambi i dispositivi. Analogie e differenze con i router con FFS.
- Gestione dei flussi di comunicazione bidirezionali tra area inside, dmz e outside dei firewall HW e tra area inside ed outside di un border/edge che collega un LAN con una WAN: flussi di livello applicativo basati su TCP ed UDP e flussi di livello 3, riconoscimento dell'origine del flusso bidirezionale tramite SPI su traffico basato su TCP, politiche empiriche per gli altri flussi ed uso/configurazione del doppio NAT process mediante le interfacce inside ed outside del firewall e del NAT router collegati tra loro.

- Uso del protocollo PPP nei diversi contesti per agganciarsi alla WAN di un ISP, autenticazione tramite PAP e CHAP.

- Uso e funzioni dei protocolli di livello applicativo KERBEROS e RADIUS in ambito LAN per AAA, generalità del protocollo IEEE 802.1x per il port-based authentication e per AAA in genere: breve analisi di EAP, EAPoL, comunicazione tra end-device e switch e tra switch e server RADIUS, ruoli/funzioni dei vari clients IEEE 802.1x(supplicant), degli switch d'accesso (authenticator) e dei sever AAA.

- Generalità dei protocolli di livello applicativo SYSLOG ed SNMPv3 per la creazione di un NMS (network management system) tra un device manager ed altri device agent, ruolo della MIB degli agent e dei messaggi get e set del manager e dei messaggi trap degli agent. Cenni agli IDS ad alla loro configurazione in rete.

Argomenti: *(parte di laboratorio)*

- Esercitazione in C.P.T. in ambito VLAN ed architettura corporate multilevel: creazione di vlan mediante porte switch e relativa comunicazione usando interfacce fisiche di router separate per ogni vlan, configurazione di porte/link in modalità access e trunk e relativi comandi per il troubleshooting, test di connettività L3 tra gli host delle vlan.
- Esercitazione in C.P.T. in ambito VLAN ed architettura corporate multilevel: creazione di vlan mediante porte switch e relativa comunicazione usando il metodo router on a stick, associando una subinterface per ogni vlan=rete ip, configurazione di porte/link in modalità access e trunk e relativi comandi per il troubleshooting, test di connettività L3 tra gli host delle vlan.
- Esercitazione in C.P.T. in ambito VLAN ed architettura corporate multilevel: creazione di vlan mediante porte switch e relativa comunicazione usando il metodo router on SVI mediante switch L3, associando una vlan interface per ogni rete ip, configurazione di porte/link in modalità access e trunk e relativi comandi per il troubleshooting, test di connettività L3 tra gli host delle vlan. Comandi specifici su switch L3 per l'attivazione del routing e per l'uso/configurazione di routed-port per la connessione in up-link verso router e relative caratteristiche.

- Estensione, in C.P.T., del sistema di reti usato per la realizzazione dell'intervlan routing su router on a stick ai fini della preparazione alla configurazione delle ACL su router: aggiunta di altre due VLAN/reti IP, una per i client e l'altra per i server e relativo test di connettività L3.

- Configurazione di ACL standard per la limitazione del traffico fra alcune VLAN/reti IP della LAN, la comunicazione fra le altre ed il mondo esterno WAN: analisi ed uso delle clausole "permit" e "deny" per la definizione delle singole ACL entry, applicazione delle ACL in entrata/uscita su interfacce L3 secondo la regola di applicazione ottimale in base alla posizione tra sorgente e destinazione. Analisi dell'algoritmo di matching con le ACL-entry e delle relazioni di inclusione tra esse, uso, significato e configurazione della regola di "implicit deny".

- Troubleshooting sulle ACL ed aggiunta/modifica delle singole ACE. Esercitazione, mediante C.P.T., sulle ACL estese applicate ad interfacce L3 su firewall integrati in configurazioni inter-vlan-routing mediante router on a stick e router on SVI/switch L3.

- Regola di ottimizzazione della bandwith/limitazione del traffico broadcast in ambito

VLAN mediante filtraggio bottom-up delle allowed vlan sui trunk in un sistema di reti con architettura corporate multilevel a due/tre livelli e relativa esercitazione in C.P.T.

- Esercitazione, in C.P.T., con la summarization statica di reti IP remote di una LAN con architettura corporate multilevel nella routing-table del router ISP (lato WAN) e relativo test di connettività L3 tra LAN e WAN.

- Creazione, mediante C.P.T., di un sistema di reti composto da tre router (collegati in modo punto-punto R1-R2-R3) e da tre rispettive LAN agganciate per la configurazione ed il test delle floating static route/backup route: preparazione del sistema mediante impostazione delle reti ip locali e di quelle remote, preferenziali ed ausiliarie, agendo sulla AD.

- Esercitazione, ad alto livello, in C.P.T, sulla configurazione del DHCP mediante un sistema di reti composto da due router collegati punto-punto e tre LAN agganciate, una per router, con relativa configurazione degli address-pool sui DHCP-server dedicati/router/switch e della option 82 su switch/ server DHCP in caso di dhcp-snooping, delle interfacce relay-agent opportune su router e del dhcp-snooping tramite porte switch untrusted e trusted.
- Collegamento e networking-configuration di un dhcp-server (IPv4 e IPv6) su un sistema di reti con architettura corporate multilayer/multilevel a due/tre livelli con intervlan routing tramite router on a stick/one arm, router on SVI, router on access-link, sia nel caso di dhcp-server esterni dedicati che in quello di dhcp-server in funzione su switch, router o firewall: configurazione delle interfacce relay agent tramite interfacce L3 fisiche, logiche/virtuali (sub-if, SVI); configurazione del dhcp-snooping, in ambito networking, in tutti i possibili casi di architettura multilevel/multilayer: impostazione delle porte untrusted e trustred e del "limit rate".

- Funzionamento dell'ARP esteso: analisi delle entry della cache ARP dei router in caso di configurazione di reti ip remote direttamente connesse nella routing table: associazioni tra mac-address locali ed ip address locali/remoti, determinazione automatica e/o non ottimale del mac-address del next-hop da usare per una directed-connected static route e relativa simulazione in C.P.T.

- Esempio semplice, in C.P.T., di un sistema di rete in cui è presente la violazione delle regole fondamentali di routing: due router adiacenti in collegamento point-to-point ma non sulla stessa rete ip e comunicanti mediante impostazione forzata delle reti ip remote sulla routing table.

- Uso e configurazione delle loopback-interface e relativa implementazione in C.P.T. mediante un sistema di reti composto da quattro router collegati in modo connesso e ridondante e delle LAN agganciate a ciascuno di essi simulate attraverso loopback-interface.

- Configurazione, mediante C.P.T., del NAT-process in overload (PAT) per tutti gli host client di una LAN stub-network con architettura corporate multilevel/multilayer con intervlan routing mediante router on a stick/router on SVI/router on access-link: definizione degli host nattabili tramite ACL-standard, uso di uno o più indirizzi nel NAT-POOL e relativo binding in overload; test di connettività L3 con host nella WAN e simulazione del tracciamento del percorso dei pacchetti IP da sorgente a destinazione, con relativa traslazione degli indirizzi IP ed uso dei comandi specifici per la visione della NAT-TABLE e dei dettagli del NAT-PROCESS sul NAT-router CISCO della LAN.

- Uso, significato e configurazione delle multiuser-connection mediante C.P.T.: analisi e configurazione dei socket utilizzati per la comunicazione tra due o più istanze di C.P.T mediante la rete reale, impostazione delle risorse di rete da condividere e delle connessioni ingoing ed outgoing, apertura e chiusura delle connessioni logiche in multiuser-connection a due a due.

Nota: le parti in blu sono state trattate in più rispetto al programma previsto nel documento del 15 maggio.

LUOGO E DATA

Bolzano, 12/06/2019

FIRMA

ALFREDO CANTARELLA