

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

PROF. **ALFREDO CANTARELLA**

CLASSE: **5•K** - anno scolastico: **2022/23**
Ore settimanali : **4 (2 di teoria + 2 di laboratorio)**

PROGRAMMA (effettivamente svolto) di: “**SISTEMI E RETI**”

Argomenti: (parte teorica)

❖ **MODULO 1 (VLAN E RETI IP):** (numero ore: 16)

UNITÀ DIDATTICHE:

SIGNIFICATO, CREAZIONE ED ISOLAMENTO DELLE VLAN, TRAFFICO TAGGATO L₂ E PROTOCOLLO IEEE 802.1Q, RELAZIONI TRA VLAN E RETI IP, SWITCH L₂ E L₃, INTER-VLAN-ROUTING, VLAN-SECURITY E BUONE NORME PER LA PROGETTAZIONE DI VLAN.

- Ripasso in sintesi della struttura di una LAN, con architettura corporate multilayer/multilevel, collegata alla WAN: uso e funzionalità del cablaggio strutturato e dei livelli di accesso, distribuzione e core/core-distribution collassato, cablaggio logico/fisico orizzontale e verticale, uso di armadi rack, patch-panel, patch-cord e joint-cord, dimensionamento di una LAN e configurazione delle relative reti IP, uso del border sulla LAN come default-gateway per gli host locali e collegamento della LAN alla WAN sul local-loop/last-mile attraverso il border-router dell'ISP di riferimento, uso, e struttura generale della routing-table e significato della default-static-route usata dal router locale.
- Introduzione alla configurazione di una rete LAN con diverse reti IP, soluzioni possibili e relative implicazioni in termini di efficienza e costi: uso di un solo router con diverse NIC fisiche (quando possibile), uso a cascata di diversi router (standard) o diversi switch multilayer/Layer 3 (L3) in collegamento punto-punto fino ad esaurimento delle reti IP e configurazione delle relative porte L3, sia nel caso di router (porte fisiche standard) che in quello di switch L3 (come porte router fisiche); uso delle interfacce di rete (NIC) virtuali/logiche come soluzione ottimale per il problema ed introduzione alla VLAN, principi d'applicazione delle NIC virtuali/logiche ed relazioni con l'uso delle VLAN (corrispondenza 1:1).
- Introduzione alla VLAN: definizione generale dei BROADCAST DOMAIN (B.D.) e, nello specifico, dei B.D. L₂ e L₃, frame broadcast espliciti ed impliciti ottenuti per flooding, analisi delle differenze/analogie, specifiche di dettaglio L₂ e L₃ e relativi esempi pratici con

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

frame e pacchetti IP. Relazione tra B.D. L3, reti IP e local/limited broadcast IP-address, separazione dei B.D. L3 ad opera dei router e relativi esempi, definizione di COLLISION DOMAIN (C.D.) / segmento di rete, uso separazione dei C.D. ad opera degli switch ma non degli HUB e relativi esempi di configurazione, definizione ed uso della microsegmentazione e relativi vantaggi. Introduzione alle VLAN ed al loro uso in ambito networking, uso e significato dei gruppi logici di host e relazioni con il subnetting IP e le [sotto]reti IP su reti fisiche, metodi di creazione delle LAN e relativa associazione degli host tramite switch o in modo autonomo: transparent-assignment, port-based-assignment, cooperative-assignment e per-user-assignment, caratteristiche fondamentali di ciascuno di tali metodi, analisi dei vantaggi/svantaggi (falsificabilità dei mac-address e degli indirizzi IP, robustezza/inviolabilità delle porte switch, inserimento di un host in più VLAN e corrispondenza 1:1 con le NIC fisiche/logiche/virtuali, indipendenza dell'utente dall'host, costi di realizzazione), breve cenno al protocollo IEEE 802.1x e relazioni col metodo port-based.

- Introduzione agli elementi fondamentali del PER USER ASSIGNMENT e al protocollo IEEE 802.1x: uso degli switch d'accesso/access point (AP) WIFI con ruolo di proxy tra lo user che deve entrare in rete e l'authentication server, blocco e sblocco logico della porta switch/radio sulla base dei pacchetti IEEE 802.1x, autorizzazione tramite user specifico ed indipendenza dell'accesso in rete dall'host, vantaggi in termini di network-security, associazione tra user/account e VLAN sull' l'authentication server, port-based assignment dinamico operato dagli switch/AP con VLAN pre-configurate o associate agli user.
- Definizioni empiriche di porte switch e link in access-mode e trunk-mode e relative definizioni esatte in ambito VLAN: uso ed analisi del traffico (dei frame) taggato e non taggato per le VLAN e di quello non taggato in assenza di VLAN e relativa struttura del frame Ethernet in entrambi i casi, valori specifici usati per mtu ed MTU ed uso del protocollo (L2) IEEE 802.1q per la gestione del tag., traffico non taggato/taggato ammesso sui link/porte in access-mode e trunk-mode, relazioni/motivazioni tra l'uso del tag IEEE 802.1q e la regola di VLAN-ISOLATION ,differenza tra tag fisico e tag logico/in RAM, applicazione e rimozione unica del tag fisico/logico nel percorso da host sorgente ad host destinazione attraverso gli switch. Uso delle VLAN come domini broadcast L2 ai fini dell'ottimizzazione della bandwidth complessiva in una rete (riduzione della circolazione dei frame broadcast espliciti ed impliciti), regole fondamentali di inclusione tra i B.D. L2 ed i B.D. L3/reti IP (prevenzione dello sconfinamento dei B.D. L2 sui B.D. L3), superamento della regola di VLAN-isolation ad opera di router/firewall, VLAN sulla stessa rete IP e relative problematiche, VLAN in corrispondenza (1:1) con le reti IP (regola di applicazione ottimale delle VLAN) e relativo filtraggio di comunicazione tramite firewall dedicato o integrato su router tramite configurazione delle ACL, uso del traffico non taggato sui trunk e della VLAN nativa, panoramica dei metodi inter-VLAN-routing (tramite router on access-link, router on a stick/one arm, router on SVI).

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 - Cadomastraße 14 St.Nr. 80006520219

- Analisi del traffico taggato (frame) in ambito VLAN, significato ed applicazione/superamento della regola di VLAN-ISOLATION da parte di switch/router e relative implicazioni per la comunicazione degli host in rete.
- Analisi ed implementazione dell'inter-VLAN-routing tramite router on access-link, vantaggi/svantaggi: uso dei link in access-mode sullo switch-core in corrispondenza (1:1) con NIC (L3) del router e relative implicazioni pratiche sul numero di interfacce di rete (L3) da usare e sulla scelta delle VLAN relative alla stessa rete IP da far comunicare fra loro.
- Uso e caratteristiche fondamentali degli switch Multilayer/L3: caratterizzazione di uno switch L3 in generale ed analisi delle differenze tecniche tra switch L3 fisici e logici, con relative implicazioni in termini SW/HW (uso di HW specializzato o meno per le SVI), sia in ambito VLAN che nell'uso di routed-port, costi ed applicazioni nelle realtà professionali avanzate.
- Analogie/differenze tra le SVI di uno switch L2 e quelle di uno switch L3 (fisico o logico) e relativi ambiti d'uso: uso del traffico di management/acceso remoto e comunicazione con server (per gli switch L2), possibilità ulteriore di fare routing tramite le VLAN interface (solo per switch L3).
- Uso e configurazione di uno switch multilayer/L3 in ambito VLAN, in una LAN con architettura corporate multilevel, sia come switch-core che come border-router per il collegamento ad una WAN: configurazione appropriata della routing-table e test di connettività L3 tra host della LAN e della WAN.
- Analisi in dettaglio delle analogie/differenze tra le sub-interface (sub-if, interfacce logiche) e le SVI (interface VLAN, interfacce virtuali): caratterizzazione su router o switch L3, associazione ad una NIC fisica o meno, valore assunto dei rispettivi mac-address ed algoritmo usato per la relativa generazione, efficienza nella gestione dell'INTER-VLAN-ROUTING tra sub-if ed SVI su Switch L3.
- Analisi in dettaglio dei vari campi del TAG IEEE 802.1q: campi TYPE/TPID, PRI, CFI e VID e relativa discussione.

❖ **MODULO 2 (FIREWALLING , ACL, ACCESSO REMOTO):** (numero ore: 9)

UNITÀ DIDATTICHE:

FIREWALL SW ED HW, ACL STANDARD ED ESTESE, PARAMETRI E CLAUSOLE SI CONFIGURAZIONE DELLE ACL, ACL INBOUND E OUTBOUND, APPLICAZIONE OTTIMALE E NON DELLE ACL E RELATIVE CONSEGUENZE, ACCESSO REMOTO AI NETWORK DEVICE TRAMITE SSH.

- Introduzione al firewalling: uso e funzionalità di un firewall per il filtro centralizzato del traffico di una LAN verso l'interno e l'esterno (WAN) anche in ambito VLAN, firewall HW/dedicati e SW e relative differenze e campi d'uso, router e switch con FFS, regole di

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

filtering/policy di sicurezza/comunicazione, definizione, uso e composizione/struttura delle ACL e delle ACL-entry e livelli dello stack TCP/IP coinvolti, proxy firewall e proxy server e relative caratteristiche/differenze, ACL standard ed extended e relativi parametri di definizione (su IPv4 ed IPv6), ACL INBOUND ed ACL OUTBOUND e relativo significato generale, applicazione multipla delle ACL ad una stessa interfaccia L3.

- Algoritmo di applicazione delle singole ACL-entry basato sul matching "if-then-else" e regola di costruzione/inserimento corretto delle singole ACL-entry per inclusione incrementale delle condizioni di riferimento, overriding dell "IMPLICIT DENY" in base alle policy di comunicazione di scelte. Analisi in dettaglio delle caratteristiche delle ACL INBOUND ed OUTBOUND in relazione all'ordine di esecuzione/applicazione rispetto alla routing-table del router/firewall di riferimento, regola universale di applicazione delle ACL standard ed extended e relative motivazioni.
- Esercitazione, in C.P.T., sulle ACL STANDARD su router con FFS in architettura corporate multilevel per il filtraggio del traffico in ambito LAN--WAN con uso di VLAN secondo specifiche policy di sicurezza/comunicazione.
- Generalizzazione sulle conseguenze dell'applicazione non ottimale (in un punto intermedio tra sorgente e destinazione IP), in modalità INBOUND ed OUTBOUND, delle ACL standard ed estese in un sistema di reti: consumo di bandwidth inutile, riduzione di prestazioni complessive del sistema per applicazione di filtri non voluti e dropping non previsto di pacchetti/frame (nei tratti sorgente IP-punto intermedio-di-applicazione e punto intermedio-di-applicazione-destinazione IP) in caso di applicazioni di filtri (ACLE) di tipo deny. Contesti d'uso reali delle ACL standard e estese.
- Ripasso ed esercitazione sull'uso delle ACL estese e sulla loro applicazione in ambito intervlan-routing tramite router on SVI per l'impostazione dei filtri di comunicazione in ambito LAN e WAN.
- Definizione ed uso dei firewall SPI e relativa applicazione con ACL extended: impostazione di traffico "established" per comunicazioni tra host basate su protocolli client-server (solo su TCP) mediante clausola specifica e relativo significato, differenze fondamentali fra i protocolli TCP (connection-oriented) e UDP (connection-less).
- Linee generali del funzionamento del protocollo SSH: richiesta di connessione, generazione e scambio della chiave simmetrica (condivisa/shared) tra client SSH e server SSH (generazione in modo random o usando l'algoritmo Diffie-Hellman), con garanzia di segretezza, autenticità e integrità, usando le chiavi RSA generate sul server SSH e sul client SSH, comunicazione tra client e server SSH usando la chiave shared e relative motivazioni.
- Analisi in dettaglio, step by step, delle varie fasi di una transazione SSH tra client e server: determinazione/accordo su versione, funzione hash ed algoritmo a chiave simmetrica da usare, scambio sicuro delle rispettive chiavi pubbliche, generazione/scambio sicuro della

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

chiave simmetrica (per la segretezza) in modalit  random (da parte del server verso il client) o tramite Diffie-Hellman (a seconda della versione SSH), inizio della sessione SSH tramite comunicazione corretta delle credenziali di accesso al server SSH da parte del client, trasmissione segreta, autentica ed integra e chiusura della sessione SSH.

❖ MODULO 2s (CRIPTOGRAFIA ED USO IN NETWORKING): (numero ore: 8)

UNIT  DIDATTICHE:

CRIPTOGRAFIA A CHIAVE SIMMETRICA ED ASIMMETRICA, SEGRETEZZA, AUTENTICIT  ED INTEGRIT  DELL'INFORMAZIONE, FUNZIONI/ALGORITMI HASH E FIRMA DIGITALE, PROTOCOLLI INTERLOCK E SSH

- Uso, applicazione ed analisi dei concetti/elementi fondamentali della crittografia moderna: crittografia a chiave simmetrica/privata/condivisa ed asimmetrica e relative analogie/differenze, uso della coppia di chiavi per criptare e decriptare da parte di ogni user (sorgente e destinatario), crittografia a chiave pubblica come caso particolare di quella asimmetrica, caratteristiche matematiche fondamentali degli algoritmi di crittografia (uso di algebra modulare ed operatori logici bit a bit) e propriet  fondamentali delle coppie chiavi (correlazione delle due chiavi, impossibilit  di ricavo di una chiave a partire dall'altra se non in tempi intrattabili esponenziali), analisi delle propriet  fondamentali della sicurezza dell'informazione in rete (segretezza/riservatezza, integrit , autenticit  e principio di non ripudio da parte del destinatario), indipendenza di tali propriet  e relativa applicazione ed esempi usando la crittografia a chiave pubblica.
- Propriet  fondamentali degli algoritmi di crittografia a chiave simmetrica ed asimmetrica in termini di complessit  temporale asintotica (polinomiale ed esponenziale rispettivamente) e principio generale, anche se non ottimale in ambito networking, per garantire contemporaneamente autenticit  ed integrit  dell'informazione trasmessa tramite algoritmi a chiave pubblica e relative motivazioni: trasmissione del dato (D)/messaggio (M)/pacchetto (P) (segreto o meno) originale concatenato allo stesso pacchetto autenticato (PK, con chiave privata del mittente A) e relativo test di autenticit  (tramite decodifica di PK con chiave pubblica di A da parte del destinatario B) ed integrit  (tramite verifica di corrispondenza tra P e PK decriptato da parte di B), analisi del conseguente decremento delle prestazioni di rete (consumo doppio della bandwidth).
- Definizione di funzione/algoritmo hash (qualsiasi) e di [message]digest/impronta, uso ed analisi delle propriet  di una buona funzione hash per l'uso in ambito crittografico: non invertibilit  (e non iniettivit ) e lunghezza fissa della digest rispetto alla dimensione dell'input (per def.), resistenza alla 1  e 2  pre-immagine, alle collisioni e relative motivazioni, lunghezze in bit delle digest per MD4 e MD5 (128), SHA1 (160), SHA-256, SHA-512, SHA-384 e relative precisioni di tali algoritmi rispetto ad un attacco del

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

compleanno. Definizione di firma digitale e relative applicazioni reali per garantire contemporaneamente in modo ottimale, in rete, autenticità ed integrità dell'informazione e relative motivazioni, uso riservato degli algoritmi a chiave simmetrica per la segretezza dei dati, uso/applicazione della firma digitale per lo scambio tra mittente e destinatario della relativa chiave simmetrica (condivisa).

- Analisi in dettaglio, step by step, delle varie fasi di una transazione SSH tra client e server: determinazione/accordo su versione, funzione hash ed algoritmo a chiave simmetrica da usare, scambio sicuro delle rispettive chiavi pubbliche, generazione/scambio sicuro della chiave simmetrica (per la segretezza) in modalità random (da parte del server verso il client) o tramite Diffie-Hellman (a seconda della versione SSH), inizio della sessione SSH tramite comunicazione corretta delle credenziali di accesso al server SSH da parte del client, trasmissione segreta, autentica ed integra e chiusura della sessione SSH.

❖ **MODULO 3 (ROUTE SUMMARIZATION E BACKUP ROUTE):** (numero ore: 8)

UNITÀ DIDATTICHE:

SUMMARY ROUTE STATICHE E DINAMICHE, ALGORITMO DI SUMMARIZATION, SUB-NETWORK E RETI SOHO, PARAMETRI DI UNA ROUTE NELLA ROUTING-TABLE E FLOATING STATIC ROUTE.

- Introduzione alla summarization di reti IP/Prefix-aggregation: significato e relazioni col subnetting IP, calcolo della rete madre ottimale/non ottimale per una serie di reti IP di partenza e relativi esempi pratici.
- Definizione ed uso/significato delle stub-network e dei stub-router: analisi delle relative proprietà ed esempi specifici reali, uso e significato delle reti SOHO, elementi/funzioni fondamentali dei protocolli FHRP per la ridondanza L3 (tramite router), delle backup-route(floating static route) e delle backup-interface in ambito stub-network.
- Analisi in dettaglio dei vari step dell'algoritmo universale per il calcolo della summary-route ottimale a partire da una serie di reti IP: individuazione delle reti IP con valore MIN e MAX, confronto bit a bit dei valori degli indirizzi IP(a partire da quello più significativo) e determinazione dei bit di matching, calcolo del NET-ID ed HOST-ID della rete IP ottimale e della relativa net-mask, necessità dell'indirizzamento classless e abbandono di quello classful, definizione di supernet ed uso del supernetting/CIDR nella realtà.
- Analisi dei campi d'uso reali e delle condizioni necessarie per la Route-Summarization su IPv4 ed IPv6, con relativo significato, e relative motivazioni: uso nei router degli ISP, Route-summarization statica (calcolo e configurazione manuale della summary-route) e dinamica (calcolo, configurazione e propagazione della summary-route ad opera dei

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

dynamic routing protocol [D.R.P.]), (precondizioni: summarization per un router e solo delle reti remote), route remote da raggruppare appartenenti ad una componente connessa del sistema di reti di cui fa parte il router corrente (IPv4 ed IPv6), contiguit  (e non continuit ) delle reti remote di cui calcolare il prefix (solo su IPv4) e relativo significato ed esempi inerenti all'indirizzamento classful standard e classless, impossibilit  di memorizzazione di tutte le reti IP del sistema di reti di una WAN, riduzione della dimensione delle routing-table in RAM ai fini della velocizzazione del processo di lookup/matching di un ip-address, riduzione del tempo di convergenza dei protocolli di routing dinamico (D.R.P.) e conseguente diminuzione del consumo di bandwidth specifica, esempi/esercitazioni di calcolo di summary-route in modalit  statica/dinamica su diversi esempi reali di sistemi di reti.

- Significato ed uso dei parametri Route Source (R.S.), distanza amministrativa (A.D.) e metrica per una route all'interno di una routing table, sia per configurazioni statiche che dinamiche tramite i dynamic routing protocol: scelta della bont  di un percorso rispetto ad un altro (AD) e relativo costo/peso (metrica), scelta del percorso migliore in ogni caso nella routing table in base ai valori di AD ed M, uso, significato e configurazione del LOAD-BALANCING dei pacchetti IP ad opera dei router e relative problematiche di networking in ambito TCP ed UDP. Uso e significato delle route di backup in ambito LAN-WAN e nelle stub-network, importanza in caso di system-failure/fault e relativa configurazione agendo sulla A.D. (administrative distance) delle route nelle routing table.

❖ **MODULO 4 (IPv4 SPECIALI/NOTEVOLI E NAT):** (numero ore: 8)

UNIT  DIDATTICHE:

USO E PROPRIET  DEI VARI INDIRIZZI IPv4 SPECIALI, IP-ADDRESS ROUTABLE E NON ROUTABLE, INDIRIZZI IP MULTICAST, INDIRIZZI IP PRIVATI, PUBBLICI E SHARED, NAT E PRINCIPI GENERALI DI FUNZIONAMENTO IN AMBITO LAN-WAN.

- Uso, analisi, ambiti d'uso di indirizzi IPv4 speciali/notevoli e relativa propriet  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 propriet  di non configurabilit  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/unicati in ambito LAN e/o WAN, motivazioni storiche legate

Repubblica Italiana Provincia Autonoma di Bolzano - Alto Adige		Republik Italien Autonome Provinz Bozen - Sdtirol
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 - Cadomastraße 14 St.Nr. 80006520219

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.

❖ **MODULO 5 (DAI, DHCP e SLAAC, elementi di FHRP):** (numero ore: 8)

UNITÀ DIDATTICHE:

DAI (Dynamic Address Information), PARAMETRI D'INDIRIZZAMENTO E CONTESTI D'USO, STATEFUL E STATELESS DAI, DHCPv4, DHCPv6 E SLAAC A CONFRONTO: ELEMENTI COMUNI DI FUNZIONAMENTO E SCENARI POSSIBILI, TRANSAZIONI DHCPv4 IN DETTAGLIO ED ANALISI DEI CAMPI, USO E CONFIGURAZIONE DI DHCP-SERVER E DI RELAY (DHCP)AGENT SU ARCHITETTURE DI RETE AD UNO PIÙ LIVELLI CORPORATE IN AMBITO VLAN, CENNI ALLA TRANSAZIONI SLAAC E DHCPv6, VIRTUAL ROUTER ED ELEMENTI FONDAMENTALI DEI PROTOCOLLI FHRP.

- Introduzione alla dynamic addressing information (DAI): 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,

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 - Cadomastraße 14 St.Nr. 80006520219

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, CIADDR, 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. -
- Elementi/condizioni fondamentali per l'uso dei protocolli FHRP e definizione/concetto di virtual-router: appartenenza alla stessa rete IP ed condivisione di un IP-address virtuale, con relativa generazione casuale di uno o più mac-address virtuali condivisi per il settaggio trasparente del/dei default-gateway sugli end-device rispetto ai fault di sistema.

❖ **MODULO 6 (NETWORK DHCP-SERVER PROTECION, MitM e DoS ATTACK):**
(numero ore: 8)

UNITÀ DIDATTICHE:

ELEMENTI GENERALI DI UN ATTACCO MITM E DoS, ESEMPI SPECIFICI E POSSIBILI SOLUZIONI, DHCP-STARVATION, DHCP- SPOOFING E RELATIVE PROBLEMATICHE, DHCP-SNOOPING E RELATIVA CONFIGURAZIONE SU SWITCH.

- 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

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

d'esecuzione, uso del port-security e del dhcp-snooping sugli switch di rete come meccanismi di difesa mediante configurazione delle porte switch in modalit  untrusted(blocked) e trusted(unblocked), filtrando il traffico delle transazioni DHCP tra client e server. Cenni all'ARP-POISONING/SPOOFING ed una possibile soluzione tramite DHCP-snooping, collegamento tra AP WIFI e switch ai fini del DHCP-Snooping.

❖ **MODULO 7 (NAT-PROCESS: CONFIGURAZIONE E PROBLEMATICHE):**
(numero ore: 8)

UNIT  DIDATTICHE:

NAT E TERMINOLOGIA SPECIFICA, TRASLAZIONE DEGLI INDIRIZZI IP TRA INSIDE ED OUTSIDE NETWORK, SNAT, DNAT, PAT, PORT-FORWARDING, NAT-POOL E NAT-HOST E RELATIVO BINDING/MAPPING, VANTAGGI E SVANTAGGI DEL NAT, NAT IN OVERLAPPING(OAT), NAT E RELAZIONE CON LE VPN E LE ACL.

- 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 pi  gradi di privacy e security mediante applicazione multipla del nat-process su uno o pi  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 cardinalit  (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

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

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.

❖ **MODULO 8 (FIREWALL, REGOLE-DMZ e NAT_DOPPIO):** (numero ore: 5)

UNITÀ DIDATTICHE:

- SPI FIREWALL, AREA DMZ E PROTEZIONE DAGLI ATTACCHI DOS, COLLEGAMENTO TRA FIREWALL, ARCHITETTURA CORPORATE –MULTILAYER/MULTILEVEL E BORDER-ROUTER IN AMBITO LAN-WAN E CONFIGURAZIONE DEL DOPPIO NAT, FLUSSI TCP/UDP BIDIREZIONALI TRA ARE INSIDE, OUTSIDE E DMZ E RELATIVA CONFIGURAZIONE.**
- 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.

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

Argomenti: *(parte di laboratorio)*

❖ **MODULO 1 (VLAN E RETI IP):** (numero ore: 15)

- Analisi e configurazione, in C.P.T., di un sistema di reti relativo ad una LAN (con architettura corporate multilevel collegata alla wan), composta da due reti IP ed host distribuiti su diversi piani, diversi switch ai piani ed un router con due interfacce IP (NIC) collegato alla WAN: configurazione degli indirizzi IP per i singoli end-device (client e server), delle route locali e remote per il router della LAN e quello dell'ISP e test di connettivit  L3 fra i vari host del sistema (locali e remoti). Significato ed uso della default static route e del default-gateway/gateway of last resort per un router e relativa configurazione, tramite C.P.T. sul border router di una LAN con architettura corporate multilevel collegata alla WAN: considerazioni sull'uso di tale route nei router sul local loop nei versi LAN-->WAN e viceversa.
- Analisi e configurazione, in C.P.T., di un sistema di reti composto da una LAN collegata alla WAN con architettura locale multilevel/multilayer a tre livelli ed implementazione delle VLAN tramite il metodo Port-Based-Assignment: creazione delle VLAN necessarie su tutti gli switch in ambito LAN e definizione/assegnazione dei vari host del sistema locale tramite porte switch alle rispettive VLAN, uso, significato e definizione/creazione delle porte switch e dei relativi link in access-mode e trunk-mode attraverso il comando CISCO IOS (di execution-level 3) "switchport" e relativi parametri.
- Uso, in C.P.T., dei comandi CISCO IOS "show vlan", "show vlan brief", "show interfaces switchport", "show interfaces trunk" e relative significato/troubleshooting su un'architettura corporate multilevel/multilayer con implementazione delle VLAN.
- Implementazione ed esercitazione, in C.P.T., sull'inter-VLAN-routing tramite router on access-link: uso dei link in access-mode sullo switch-core in corrispondenza (1:1) con NIC (L3) del router e relative implicazioni pratiche sul numero di interfacce di rete (L3) da usare e sulla scelta delle VLAN relative alla stessa rete IP da far comunicare fra loro.
- Esercitazione, in C.P.T., sull'uso del traffico (dei frame) taggato in ambito VLAN e della relativa regola di VLAN-ISOLATION da parte di switch e router e relative implicazioni per la comunicazione degli host in rete, uso dell'ambiente "simulation" del workspace del simulatore C.P.T. per l'analisi dei frame lungo il percorso da host sorgente ad host destinazione in relazione alla VLAN di provenienza e all'applicazione della VLAN-ISOLATION-RULE con relativa visione/analisi della mac-address-table degli switch in ambito VLAN (colonna VLAN sorgente/di apprendimento del mac-address di un host nella tabella) per l'applicazione della suddetta regola.

Repubblica Italiana Provincia Autonoma di Bolzano - Alto Adige		Republik Italien Autonome Provinz Bozen - Sdtirol
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

- Analisi ed implementazione/configurazione, in C.P.T., di un sistema di reti composto da una LAN collegata alla WAN con architettura locale multilevel/multilayer a tre livelli ed implementazione delle VLAN tramite il metodo Port-Based-Assignment: uso della regola d'uso ottimale delle VLAN mediante associazione con cardinalità (1:1) con le rispettive reti IP della LAN, uso di reti IP = VLAN separate per gli host client e server, configurazione dei vari HOST del SISTEMA DI RETI secondo lo schema di indirizzamento specificato, sia nella parte LAN che nella parte WAN, configurazione delle reti IP LOCALI e REMOTE, definizione dei relativi link/porte switch in access-mode o trunk-mode e preparazione del link tra lo switch core ed il router della LAN per l'INTER-VLAN-ROUTING tramite ROUTER ON A STICK/ON ARM.
- Implementazione, attraverso C.P.T., in un sistema di reti composto da una LAN, con architettura corporate multilevel/multilayer a tre livelli, collegata alla WAN, del metodo INTER-VLAN-ROUTING tramite router on a stick/on arm per il veicolamento del traffico tra le VLAN e verso la WAN: uso delle interfacce "sub-interface(sub-if)" come interfacce logiche/virtuali sul border router della LAN, associazione delle VLAN alle rispettive sub-if e relative convenzioni adottate, definizione delle reti IP associate alle sub-if e visione del contenuto aggiornato della routing-table tramite comando Cisco IOS "show ip route", configurazione del link tra lo switch core ed il border-router in trunk-mode e relative motivazioni, uso dei comandi "show vlan brief" ed "show interfaces trunk".
- Analisi, attraverso C.P.T., in real time e simulation, del traffico taggato e non taggato in un sistema di reti composto da una LAN, con architettura corporate multilevel/multilayer a tre livelli, collegata alla WAN, con INTER-VLAN-ROUTING tramite router on a stick/on arm per il veicolamento del traffico tra le VLAN e verso la WAN: analisi di alcuni campi fondamentali del tag IEEE 802.1q (TPID, VID) dei frame Ethernet lungo il percorso sorgente-destinazione attraverso i link d'accesso e i trunk, uso del tag in RAM, del tag fisico e della VLAN NATIVA, confronto tra il VID applicato da switch e router e superamento della VLAN-ISOLATION RULE ad opera dei router (uso della vlan sorgente/destinazione), analisi delle proprietà fondamentali delle "sub-interface(sub-if)" dei router (uso nei router, associazione/generazione a partire da un'interfaccia fisica e valore dei MAC-ADDRESS usati), uso dei comandi CISCO IOS "show interfaces" e "show ip interface" con gli appropriati argomenti per la visualizzazione delle proprietà fondamentali delle (sub)-interface ed eventuale troubleshooting.
- Esercitazione in C.P.T. sul traffico taggato e non taggato in ambito VLAN con intervlan-routing tramite router on a stick/on arm: uso del tag in RAM, tag fisico e della VLAN NATIVA applicato da switch e router per la VLAN-ISOLATION-RULE, proprietà fondamentali delle subinterfacce.
- Implementazione, attraverso C.P.T., in un sistema di reti composto da una LAN, con architettura corporate multilevel/multilayer a tre livelli, collegata alla WAN, del metodo INTER-VLAN-ROUTING tramite router on SVI/"VLAN INTERFACE" con switch L3 fisico per il veicolamento del traffico tra le VLAN e verso la WAN : uso delle "interface

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 - Cadomastraße 14 St.Nr. 80006520219

VLAN" come interfacce virtuali sullo switch multilayer/L3 collegato al border-router della LAN, associazione implicita delle interfacce VLAN alle rispettive VLAN, definizione delle reti IP associate alle singole VLAN INTERFACE, abilitazione del routing IP e visione del contenuto aggiornato della routing-table tramite comando Cisco IOS "show ip route", configurazione del protocollo di tagging/encapsulation dei frame sui trunk dello switch multilayer usato come core e del link tra lo switch core ed il border-router in modalità punto-punto, uso e configurazione delle "routed port" e relative caratteristiche e motivazioni per il collegamento up-link dello switch L3 con un router.

- Analisi, in C.P.T., della mac-address-table e della routing-table di uno switch L3 in presenza di SVI, analisi ed analogie/differenze del tagging dei frame in entrata/uscita sui link d'accesso e trunk tra gli switch e relazioni con la VLAN-ISOLATION-RULE, test di connettività tra gli host appartenenti alla stessa VLAN ed a VLAN diverse.
- Proprietà/caratteristiche fondamentali delle routed- port: inapplicabilità dei protocolli di STP e di link-aggregation, non divisibilità in sub-if e relative motivazioni.
- Algoritmo fondamentale eseguito da uno switch L3 (fisico o logico) per individuare l'outgoing-interface L2 (=porta switch d'uscita) per un frame Ethernet indirizzato ad un host locale in ambito VLAN con INTERVLAN-ROUTING tramite ROUTER ON SVI: ricezione dei frame con mac-address destinazione appartenente ad una VLAN-INTERFACE dello switch, controllo dello stato attivo dell'IP-ROUTING, lookup/matching dell'ip-address destinazione nella routing-table e determinazione della VLAN-INTERFACE d'uscita e del relativo tagging, individuazione della corrispondente porta switch L2 a partire dal mac-address destinazione locale usando la mac-address-table. Controllo di tale algoritmo con C.P.T in modalità simulation mediante analisi dei frame lungo il percorso sorgente-destinazione, della routing table e della mac-address-table dello switch L3.
- Esercitazione a gruppi in C.P.T, sull'INTERVLAN ROUTING tramite ROUTER ON SVI.
- Implementazione, attraverso C.P.T., del filtro (L2) delle VLAN lecite/ammissibili sui trunk (per ogni side) presenti in un sistema di reti composto da una LAN, con architettura corporate multilevel/multilayer a tre livelli, collegata alla WAN, qualunque sia il metodo INTER-VLAN-ROUTING implementato: analisi del traffico (lecito/ammissibile di VLAN) ascendente sull'albero di copertura tra switch e considerazione sul traffico discendente sullo stesso albero in relazione alla modalità di tagging dei frame in ambito VLAN da parte del router, ai fini delle impostazioni delle VLAN lecite per ogni trunk, usando il comando Cisco IOS "switchport" coi parametri di pertinenza; test di connettività L3 tra gli host delle varie VLAN, sia in REAL-TIME che in SIMULATION.

❖ **MODULO 2 (FIREWALLING , ACL, ACCESSO REMOTO):** (numero ore: 9)

- Esercitazione, in C.P.T., sulla configurazione delle ACL standard sul firewall integrato del

Repubblica Italiana Provincia Autonoma di Bolzano - Alto Adige		Republik Italien Autonome Provinz Bozen - Sdtirol
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

border router (router con FFS) di una LAN con architettura corporate multilevel/multilayer con INTER VLAN ROUTING tramite ROUTER ON A STICK: definizione di una più policy di comunicazione/security e delle relative ACL standard per il blocco/negazione del traffico tra certe VLAN fra loro e tra alcune VLAN e la WAN, ACL numbered ed named e relative convenzioni su IPv4 ed IPv6, uso delle clausole "permit" e "deny", delle netmask inverse (wildcard-mask) e relative motivazioni, delle parole chiave "any" ed "host" per la specifica di un generica rete/indirizzo IP (0.0.0.0/0) o di un host singolo specifico (/32), regola universale di applicazione delle ACL standard e relative motivazioni, applicazione delle ACL standard in INBOUND o OUTBOUND su una singola interfaccia L3 (interfacce logiche/subinterfacce e fisiche del border router), uso e significato dell'entry "IMPLICIT DENY" e relative motivazioni, test di connettività L3 tra gli host del sistema per la verifica delle policy di comunicazione/sicurezza impostate.

- Esercitazione, in C.P.T., sulla configurazione delle ACL extended sui firewall integrati dello switch core multilayer e del border router (switch L3/router con FFS) di una LAN con architettura corporate multilevel/multilayer con INTER VLAN ROUTING tramite ROUTER ON SVI: definizione di una più policy di comunicazione/security e delle relative ACL extended per il blocco/permesso del traffico di rete tra certe VLAN ed host specifici, tra alcune VLAN e la WAN, sia in termini di pacchetti generici, che in termini di pacchetti specifici attraverso l'impostazione di filtri su certi protocolli di livello network e/o transport ed applicativo usando opzionalmente i numeri di porta logica dei relativi servizi specifici in rete (http/https, DNS, ecc); applicazione ottimale delle ACL extended in modalità INBOUND -OUTBOND sulle rispettive interfacce SVI (interface VLAN) dello switch core e sull'interfaccia WAN del border router.
- Applicazioni, in C.P.T., delle ACL-extended per il filtraggio di traffico "established", su una architettura corporate multilevel, tra client e server di una rete LAN e relative applicazioni nella realtà.
- Configurazione, tramite C.P.T., degli switch e router per l'accesso [da] remoto tramite SSH in un sistema di reti con architettura corporate multilevel/multilayer: uso e significato delle porte VTY, uso dei comandi CISCO IOS "hostname" e "ip domain-name" per la definizione del nome-host e del nome di dominio, "username" (coi relativi argomenti) per la definizione degli account locali per l'accesso remoto, "crypto key generate RSA" per l'attivazione del server SSH e la definizione della coppia di chiavi RSA correlate, "transport input ssh" e "login local" su porte VTY per l'abilitazione degli accessi da remoto con SSH tramite account locale. Configurazione, in C.P.T, degli accessi remoti SSH ai network-device protetti (filtro sulle reti IP di provenienza, ecc ..., dalla parte interna/trust della rete LAN e dalla parte esterna/WAN) tramite uso/setting di filtri con ACL standard/extended e relativa applicazione sulle porte virtuali VTY mediante comando Cisco IOS "access-class" e relativi argomenti. Prova d'accesso [da] remoto tramite SSH da un end-device verso gli switch e router del sistema di reti configurato e trasferimento [da] remoto di file di configurazione di

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 - Cadomastraße 14 St.Nr. 80006520219

rete e/o immagini binarie di O.S. per switch/router di OS su un server remoto TFTP/FTP remoto collegato al sistema di reti dato.

- Uso e configurazione, in C.P.T., del traffico ESTABLISHED (su flussi TCP) attraverso le ACL EXTENDED e relativi esempi su RETI ed APPLIAZIONI REALI.

❖ **MODULO 3 (ROUTE SUMMARIZATION E BACKUP ROUTE):** (numero ore: 9)

- Configurazione, mediante C.P.T., delle floating-static-route in un sistema di reti composto da tre router collegati in modalità punto-punto e tre rispettive LAN agganciate e relativo test di connettività L3: analisi della routing-table e del comportamento delle route di backup di quelle master/principali in seguito a simulazioni di system failure (problemi di cablaggio, guasto di NIC, ecc ...).
- Configurazione, tramite C.P.T. di floating static routes in un sistema di reti composto da tre router e tre LAN collegate, una per router agendo sulla AD e relativo comportamento delle routing-table in caso di system-fault.

❖ **MODULO 5 (DAI, DHCP e SLAAC, elementi di FHRP):** (numero ore: 5)

❖ **MODULO 6 (NETWORK DHCP-SERVER PROTECION, MitM e DoS ATTACK):** (numero ore: 4)

- 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 trusted e del "limit rate".

❖ **MODULO 7 (NAT-PROCESS: CONFIGURAZIONE E PROBLEMATICHE):**
(numero ore: 4)

- Configurazione, in C.P.T., del NAT PROCESS , in modalità statica (SNAT) e dinamica (DNAT) nelle quattro varianti/casi possibili (SNAT puro, DNAT puro, DNAT con

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 - Cadomastraße 14 St.Nr. 80006520219

OVERLOAD/PAT, SNAT con OVERLOAD/PORT FORWARDING) su una LAN con un'architettura corporate multilayer/multilevel: uso e configurazione sul NAT-ROUTER sulla LAN, in base ai diversi casi, degli inside local address ed inside global address, outside local address ed outside global address (nel caso di OAT/NAT IN OVERLAPPING) in corrispondenza/cardinalità (1:1), (m:m), (m:1) tra loro tramite individuazione/creazione dei NAT-HOST sulla LAN (al variare delle diverse VLAN, tramite ACL standard o singolarmente), definizione dei corrispondenti NAT-POOL e binding/mapping tra i corrispondenti NAT-HOST e NAT-POOL nella NAT-TABLE, uso e definizione delle interfacce INSIDE ed OUTSIDE del NAT-ROUTER e visione del contenuto del NAT-TABLE tramite comandi CISCO IOS corrispondenti, ai fini del network troubleshooting.

- Ridefinizione, in C.P.T., del contenuto della ROUTING-TABLE del BORDER-ROUTER dell'ISP sulla base della configurazione del NAT PROCESS applicato al NAT-ROUTER sulla LAN: rimozione delle vecchie ROUTE destinazione (della rete LAN) con valori di IP address privato (non più valide) e configurazione delle nuove ROUTE destinazione mediante gli INSIDE GLOBAL ADDRESS (pubblici o privati), disposti dal provider /ISP, con netmask /32 o meno (a seconda del tipo di NAT usato sul NAT-ROUTER sulla LAN) e raggiungibili puntando (come next-hop) al NAT-ROUTER della LAN.
- Test di connettività L3 e L4-L5, in C.P.T., tra gli host della LAN e quelli della WAN dopo aver configurato il NAT-PROCESS sul NAT-ROUTER della LAN e ridefinito la ROUTING-TABLE del BORDER-ROUTER dell'ISP, sia in REAL TIME che in SIMULATION MODE, e relativa presa visione delle TRASLAZIONI NAT attive applicate lungo il percorso tra host sorgente e destinazione.

LUOGO E DATA

FIRMA

Bolzano, 10/06/2023

ALFREDO CANTARELLA

