Sistemi e Reti
Svolgimento Seconda Prova d'Esame
Sessione Suppletiva 2018

Leone Matteo Pio V L

12 aprile 2024

Indice

1 Prima Parte - Punto 1

1.1 Progetto Grafico dell'architettura dell'infrastruttura di rete

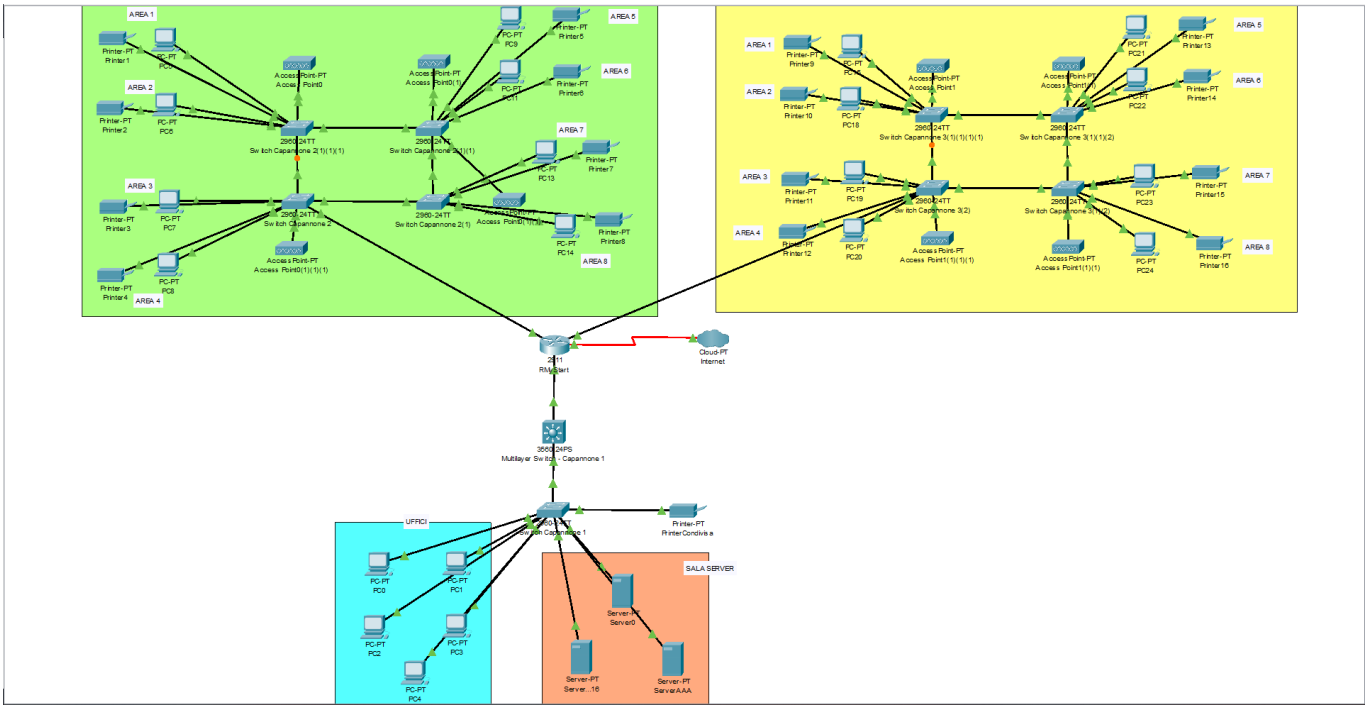

Figura 1: Progetto Grafico

1.1.1 Descrizione e Ipotesi

Per lo il mio svolgimento, della traccia d'esame, ho innanzitutto suddiviso il progetto reale in tre capannoni (distanti tra loro intorno ai 100 metri), e collegati tutti ad Internet. Per prima cosa ho predisposto un Router 2911 della Cisco come Router principale dell'azienda MyStart, che gestisce la connessione interna e la connessione ad Internet. Qui si possono formulare le seguenti ipotesi:

- VPN per rendere sicura la comunciazione fuori dall'azienda;
- ACL nel Router che "fa" da Firewall;
- Rotte.

Per il primo capannone, ho usufruito di uno Switch L3 (per gestire l'intervlan), connesso ad uno Switch L2 da 24 Porte, che connette i 5 Uffici con 1 PC ciascuno, una stampante condivisa e la Sala Server una per ogni Startup. Qui si possono formulare le seguenti ipotesi:

- Indirizzamento IP Privati tramite DHCP, usando server, per tutti i dispositivi ES, tranne per i Server che hanno bisogno di un Indirizzo IP Statico;
- VLAN per gli Uffici e VLAN per la Sala Server;
- NAT Dinamico degli Uffici e NAT Statico per i Server, per la comunicazione fuori LAN;

- Rotta Dinamica che annuncia le due LAN (Uffici, Sala Server);
- Login Local nello Switch sia nella Line Console che nella Line Virtuale;
- Port Security.

Per il secondo capannone, ho usufruito di uno Switch L3 (per gestire l'intervlan), connesso a due Switch L2 da 48 Porte, a causa dei 64 dispositivi presenti, siccome c'è la presenza di 8 aree (una per ogni Startup). Ogni area ha 8 computer, una stampante condivisa e 16 dispositivi mobili, dunque collegato allo Switch abbiamo anche un Access Point (uno per area) che fornisce connessione Wireless. Qui si possono formulare le seguenti ipotesi:

- Indirizzamento IP Privati tramite DHCP, usando server, per tutti i dispositivi ES;
- VLAN per ogni area;
- NAT Dinamico, per la comunicazione fuori LAN;
- Rotta Dinamica che annuncia le aree;
- Login Local nello Switch sia nella Line Console che nella Line Virtuale;
- Port Security;
- Configurazione dell'AP.

Per il terzo capannone, ho usufruito di uno Switch L3 (per gestire l'intervlan), connesso a due Switch L2 da 48 Porte, a causa dei 64 dispositivi presenti, siccome c'è la presenza di 8 aree (una per ogni Startup). Ogni area ha 8 computer, una stampante condivisa e 16 dispositivi mobili, dunque collegato allo Switch abbiamo anche un Access Point (uno per area) che fornisce connessione Wireless. Qui si possono formulare le seguenti ipotesi:

- Indirizzamento IP Privati tramite DHCP, usando server, per tutti i dispositivi ES;
- VLAN per ogni area;
- NAT Dinamico, per la comunicazione fuori LAN;
- Rotta Dinamica che annuncia le aree;
- Login Local nello Switch sia nella Line Console che nella Line Virtuale;
- Port Security;
- Configurazione dell'AP.

1.2 Le Risorse Hardware e Software Necessarie

Per lo svolgimento della traccia ho usato le seguenti risorse Hardware:

- 1 Router 2911 della Cisco;
- 3 Switch L3 della Cisco (uno a capannone);
- 4 Switch L2, della Cisco, da 48 Porte (per i capannoni con le 8 aree);

- 1 Switch L2, della Cisco, da 24 Porte (per i capannoni con l'Uffici e la Sala Server);
- 16 Server per i servizi delle Startup e 1 Server AAA;
- 16 Access Point per la connessione Wireless.

Come Software ho utilizzato:

- Per i Server: Linux Centos.

1.3 Piano di Indirizzamento

Per l'assegnamento degli indirizzi IP, utilizzo un Server DHCP, per l'assegnamento automatico degli indirizzi, tranne per la sala Server, che hanno necessita di indirizzi IP Statici. Per prima cosa definiamo le VLAN:

VLAN	Indirizzo IP	Nome
10	192.168.1.0\24	vlan_Uffici
20	192.168.2.0\24	vlan_SalaServer
30	192.168.3.0\24	vlan_Area1_Capannone2
40	192.168.4.0\24	vlan_Area2_Capannone2
50	192.168.5.0\24	vlan_Area3_Capannone2
60	192.168.6.0\24	vlan_Area4_Capannone2
70	192.168.7.0\24	vlan_Area5_Capannone2
80	192.168.8.0\24	vlan_Area6_Capannone2
90	192.168.9.0\24	vlan_Area7_Capannone2
100	192.168.10.0\24	vlan_Area8_Capannone2
110	192.168.11.0\24	vlan_Area1_Capannone3
120	192.168.12.0\24	vlan_Area2_Capannone3
130	192.168.13.0\24	vlan_Area3_Capannone3
140	192.168.14.0\24	vlan_Area4_Capannone3
150	192.168.15.0\24	vlan_Area5_Capannone3
160	192.168.16.0\24	vlan_Area6_Capannone3
170	192.168.17.0\24	vlan_Area7_Capannone3
180	192.168.18.0\24	vlan_Area8_Capannone3

Andiamo poi a definire gli indirizzi IPv4 nei vari capannoni. Nel capannone 1 abbiamo (i ... stanno a significare che esistono altri dispositivi uguali, nella config, non scritti):

Dispositivo	Indirizzo
PC1	192.168.1.x\24
PC2	192.168.1.x\24
PC3	192.168.1.x\24
PC4	192.168.1.x\24
PC5	192.168.1.x\24
Server1	192.168.2.x\24
Server2	192.168.2.x\24
...	...
Server16	192.168.2.x\24
ServerAAA	192.168.2.x\24

Nel capannone 2 e 3 (visto che abbiamo li stessi dispositivi) abbiamo (i ... stanno a significare che esistono altri dispositivi uguali, nella config, non scritti):

Dispositivo	Indirizzo
Stampante1	192.168.3.x\24
PC1	192.168.3.x\24
Stampante2	192.168.4.x\24
PC2	192.168.4.x\24
Stampante3	192.168.5.x\24
PC3	192.168.5.x\24
Stampante4	192.168.6.x\24
PC4	192.168.6.x\24
Stampante5	192.168.7.x\24
PC5	192.168.7.x\24
Stampante6	192.168.8.x\24
PC6	192.168.8.x\24
Stampante7	192.168.9.x\24
PC7	192.168.9.x\24
Stampante8	192.168.10.x\24
PC8	192.168.10.x\24

1.4 Caratteristiche del Collegamento ad Internet

Per il collegamento nelle reti LAN, ho impiegato cavi Ehternet di categoria gigabit per collegare gli switch, mentre tra i dispositivi ho utilizzato cavi FastEthernet. Per quanto riguarda la connessione tra le reti LAN, ho optato per una connessione ad alta velocità tramite fibra ottica per assicurare elevate performance.

1.5 Soluzioni Possibili per Assicurare la Continuità del Servizio

Per mantenere un servizio continuo, potremmo introdurre sistemi di backup e ridondanza per i server. Questo potrebbe includere l'implementazione di più router e switch per assicurare che il servizio non venga interrotto in caso di guasti hardware o problemi di rete.

2 Prima Parte - Punto 2

2.1 Tecniche per Proteggere ciascuna Start-Up da Accessi non Autorizzati

Per la protezione da accessi non autorizzati, delle varie StartUp, presenti nell'azienda, possiamo utilizzare varie soluzione come:

- Uso di Port-Security per evitare attacchi;
- Uso di un Firewall con access-list (cioè regole definite), per gestire il traffico;
- Uso delle VLAN, isolando in modo efficace il traffico di ciascuna start-up.

2.2 Principali Servizi di Rete Necessari

Tra i vari servizi di rete necessari (tra cui ad es. identificazione degli utenti, assegnazione della configurazione di rete ai vari client, risoluzione dei nomi, ...), prendiamo in considerazione (nel nostro caso), i servizi:

- DHCP: Assegnamento automatico degli indirizzi;
- DNS: Risoluzione dei nomi di dominio in indirizzi IP.

Andiamo a descrivere la configurazione del DHCP, che presenta i seguenti comandi:

DHCP.pkt

```
ip DHCP pool [poolName];
network [Ip della Rete] [SubnetMask];
default-router [Ip Default-Gateway].
```

2.3 Soluzioni per Consentire alle Start-Up la Gestione dei Propri Servizi Mediante Accesso Remoto ai Server

Per consentire alle StartUp la gestione dei propri servizi, anche da Remoto (tramite protocolli software), possiamo utilizzare almeno due possibili soluzioni:

- Utilizzo del protocollo SSH (o Telnet quasi deprecato), che permette di stabilire una sessione remota cifrata;
- Uso di VPN per connettersi in modo sicuro e remoto ai server.

3 Seconda Parte - Punto IV

Cifratura Simmetrica

La crittografia simmetrica è un metodo crittografico che utilizza una singola chiave per sia la cifratura che la decifratura dei dati. Alcuni degli algoritmi più comuni utilizzati per la crittografia simmetrica includono AES, 3DES e IDEA. Questi algoritmi sono ampiamente utilizzati per garantire la sicurezza e la riservatezza delle informazioni attraverso la crittografia dei dati.