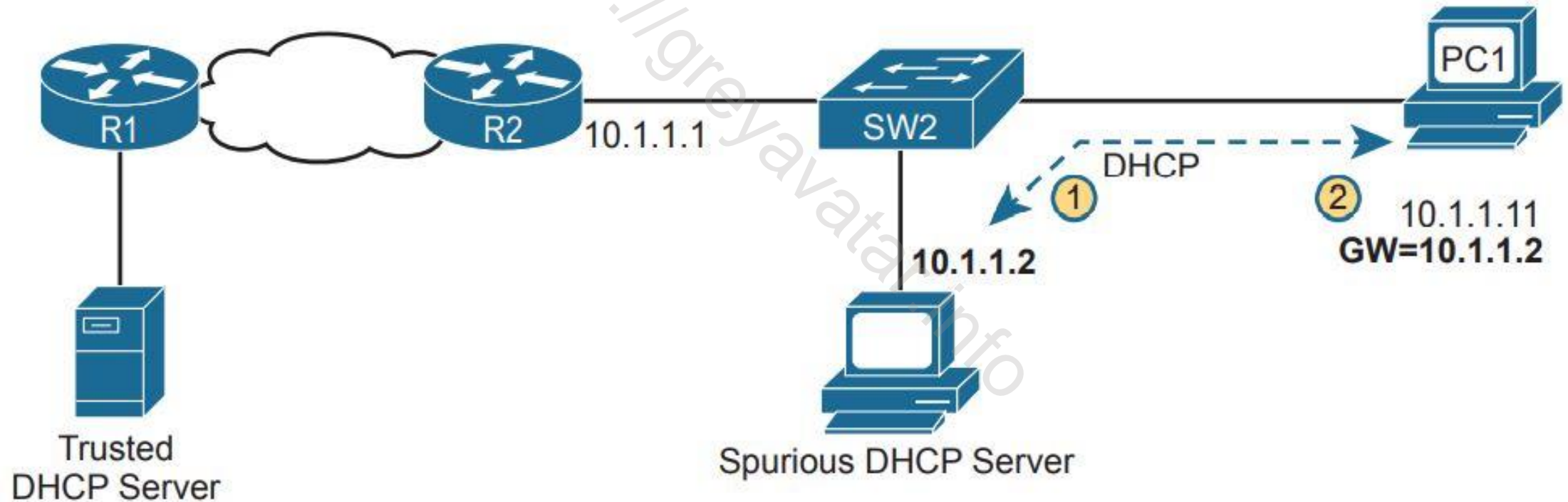


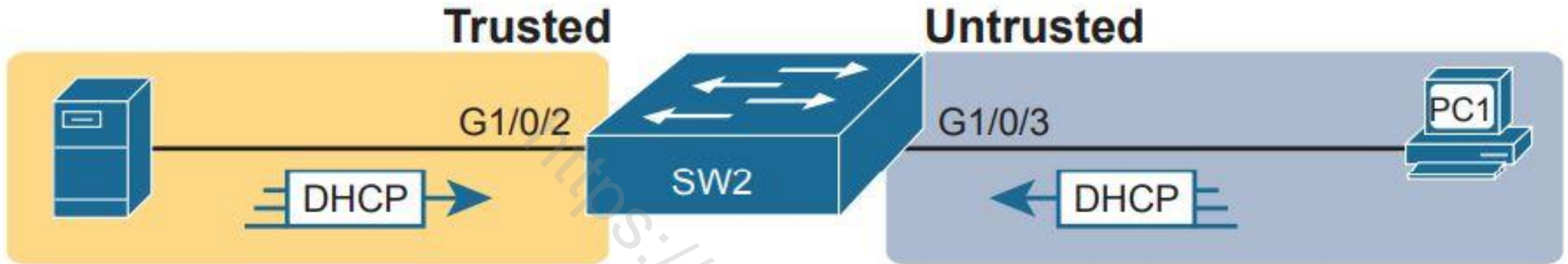
# CCNA 200-301 DHCP SNOOPING

---

INTRODUZIONE

- L'immagine mostra un attacco nel quale un attaccante agisce simulando il comportamento di un server DHCP. Notare che il **gateway** per il client sarà l'indirizzo IP dell'attaccante.





DHCP All Messages: **Approved!**

DHCP **Server** Messages: **Rejected!**

DHCP **Client** Messages:

- A) Check DISCOVER MAC Addresses
- B) Check RELEASE/DECLINE

- A livello di switch posso attivare la funzione DHCP Snooping per indicare su quali porte è corretto ricevere i messaggi del protocollo inviati dal server, se i messaggi del server non arrivano da una porta trusted vengono scartati.

# MESSAGGI DHCP

---

- Client: DISCOVER, REQUEST, RELEASE, DECLINE
- Server: OFFER, ACK

Oltre ai messaggi di Discover e Request il client invia:

- Release: per rilasciare l'ip assegnato del quale non ha più bisogno
- Decline: per non accettare un'offerta di IP inviata durante il normale flusso del protocollo(DORA)

# DHCP SNOOPING RULES

---

1. Analizza tutti i messaggi in ingresso.
2. Di default scarta i messaggi inviati dal server
3. Se il messaggio è inviato dal client filtra come segue
  1. Per DISCOVER e REQUEST, controlla la consistenza tra MAC address e messaggio DHCP
  2. Per RELEASE e DECLINE, controlla l'interfaccia di arrivo e confronta l'indirizzo IP con la tabella DHCP Snooping binding
4. Per i messaggi non filtrati che portano al lease di un IP, si costruisce una nuova riga di tabella DHCP snooping binding

# DHCP SNOOPING CONFIGURATION

---

1. Entrambi i comandi sono richiesti:
  1. Usa **ip dhcp snooping** comando globale per abilitare DHCP Snooping sullo switch.
  2. Usa **ip dhcp snooping vlan vlan-list** comando globale per selezionare le VLANs sulle quali usare DHCP Snooping.
  3. (Opzionale): Usa **no ip dhcp snooping information option** comando globale sugli switch Layer 2 per disabilitare l'inserimento del DHCP opzione 82 dei messaggi DHCP, in modo specifico sugli switches che non operano come DHCP relay agent.
2. Configurare **ip dhcp snooping trust** sottocomando di interfaccia per sovrascrivere l'impostazione di default (not trusted).
3. (Opzionale): DHCP Snooping rate limits e err-disabled recovery:
  1. (Opzionale): Configura **ip dhcp snooping limit rate numero** sottocomando di interfaccia per settare un limite dei messaggi DHCP per second.
  2. (Opzionale): Configura **errdisable recovery cause dhcp-rate-limit** comando globale per abilitare il ripristino automatico dopo che l'interfaccia viene disabilitata a causa di errore per lo sfioramento del rate-limit
  3. (Opzionale): Configura **errdisable recovery interval seconds** comando globale per settare un periodo di attesa prima di ripristinare l'interfaccia dopo un err-disable indipendentemente dalla causa