CAPITOLO 9 – PROGETTAZIONE, MONITORAGGIO E TROUBLESHOOTING DELLE RETI

Obiettivi del Capitolo

Al termine di questo capitolo il corsista sarà in grado di:

- Comprendere le fasi della progettazione di una rete.
- Identificare i requisiti di una infrastruttura di rete.
- Applicare metodologie di troubleshooting.
- Utilizzare i principali strumenti di diagnostica.
- Analizzare problemi di connettività.
- Comprendere i principi del monitoraggio delle reti.
- Interpretare indicatori di prestazione e disponibilità.

9.1 Introduzione alla progettazione di rete

La progettazione di una rete consiste nella definizione dell'infrastruttura necessaria per soddisfare le esigenze operative di un'organizzazione.

Una rete ben progettata deve garantire:

- prestazioni adeguate;
- sicurezza;
- affidabilità;
- scalabilità;
- semplicità di gestione.

Una progettazione errata può causare problemi continui e costi elevati nel tempo.

9.2 Analisi dei requisiti

Prima di progettare una rete è necessario raccogliere informazioni.

Requisiti funzionali

Descrivono cosa la rete deve consentire.

Esempi:

- accesso a Internet;
- condivisione file;
- videoconferenze;
- accesso ai servizi cloud.

Requisiti non funzionali

Descrivono il livello qualitativo richiesto.

Esempi:

- disponibilità;
- sicurezza;
- velocità;
- affidabilità.

9.3 Dimensionamento della rete

Il progettista deve valutare:

- numero utenti;
- dispositivi collegati;
- server;
- stampanti;
- telefoni IP;
- dispositivi IoT.

Una stima corretta consente di evitare colli di bottiglia futuri.

9.4 Scalabilità

Una rete deve poter crescere nel tempo.

Occorre prevedere:

- aumento utenti;
- nuove sedi;
- nuovi servizi;
- crescita del traffico.

Una rete progettata solo per le esigenze attuali rischia di diventare rapidamente insufficiente.

9.5 Progettazione gerarchica

Nelle reti aziendali moderne viene spesso utilizzato un modello gerarchico.

Core Layer

Backbone principale.

Garantisce elevata velocità.

Distribution Layer

Gestisce routing e politiche di rete.

Access Layer

Collega utenti e dispositivi finali.

9.6 Documentazione della rete

Una rete professionale deve essere documentata.

La documentazione include:

- diagrammi;
- indirizzamento IP;
- configurazioni;

- inventario dispositivi;
- procedure operative.

Una documentazione aggiornata riduce i tempi di intervento.

9.7 Introduzione al Troubleshooting

Troubleshooting significa:

ricerca e risoluzione dei problemi.

È una delle attività più importanti per gli amministratori di rete.

9.8 Approccio metodologico

Uno degli errori più comuni consiste nell'intervenire senza una metodologia.

Un approccio corretto prevede:

1. Identificazione del problema.
2. Raccolta informazioni.
3. Formulazione delle ipotesi.
4. Verifica delle ipotesi.
5. Risoluzione.
6. Validazione finale.
7. Documentazione.

9.9 Utilizzo del modello OSI nel troubleshooting

Il modello OSI rappresenta uno strumento molto efficace per individuare la causa dei problemi.

Approccio tipico:

Livello 1 → Verifica cavi e collegamenti.

Livello 2 → Verifica switch e MAC Address.

Livello 3 → Verifica IP e routing.

Livello 4 → Verifica TCP/UDP.

Livello 7 → Verifica applicazioni.

9.10 Problemi del livello fisico

Sintomi tipici:

- assenza di connessione;
- LED spenti;
- disconnessioni frequenti.

Cause comuni:

- cavi danneggiati;
- connettori difettosi;
- porte guaste;
- interferenze.

9.11 Problemi del livello Data Link

Sintomi:

- collisioni;
- errori Ethernet;
- VLAN errate.

Cause:

- configurazioni errate;
- switch mal configurati;
- loop di rete.

9.12 Problemi del livello Network

Sintomi:

- impossibilità di raggiungere altre reti;
- accesso a Internet non disponibile.

Cause:

- IP errato;
- subnet mask errata;
- gateway errato;
- routing non corretto.

9.13 Problemi DNS

Uno dei problemi più frequenti.

Sintomo:

l'utente non riesce ad aprire siti web tramite nome.

Esempio:

www.esempio.it non funziona

ma

192.168.x.x funziona.

Questo indica generalmente un problema DNS.

9.14 Il comando Ping

Ping è uno degli strumenti più utilizzati.

Utilizza il protocollo ICMP.

Permette di verificare:

- raggiungibilità;
- latenza;
- continuità della connessione.

Esempio

ping 8.8.8.8

Se il sistema risponde significa che la destinazione è raggiungibile.

9.15 Interpretazione del Ping

Output tipico:

Reply from 8.8.8.8

Time = 20 ms

TTL = 117

Time

Indica la latenza.

TTL

Time To Live.

Limita il numero di router attraversabili.

9.16 Traceroute

Traceroute consente di visualizzare il percorso seguito dai pacchetti.

Su Windows:

tracert

Su Linux:

traceroute

Utilità

Permette di individuare:

- router problematici;
- interruzioni di percorso;
- elevata latenza.

9.17 Ipconfig

Comando disponibile nei sistemi Windows.

Mostra:

- indirizzo IP;
- subnet mask;
- gateway;
- DNS.

Esempio

ipconfig

oppure

ipconfig /all

9.18 Ifconfig e IP

Nei sistemi Linux si utilizzano:

ifconfig

oppure

ip addr

Permettono di visualizzare le configurazioni delle interfacce di rete.

9.19 Nslookup

Nslookup consente di verificare il funzionamento del DNS.

Esempio:

nslookup www.openai.com

Il comando restituisce l'indirizzo IP associato al dominio.

9.20 Netstat

Netstat mostra:

- connessioni attive;
- porte aperte;
- stato delle connessioni.

È utile per individuare:

- problemi applicativi;
- servizi in ascolto;
- attività sospette.

9.21 Monitoraggio della rete

Monitorare una rete significa controllarne continuamente lo stato.

Obiettivi:

- individuare anomalie;
- prevenire guasti;
- migliorare le prestazioni.

9.22 Indicatori di prestazione

Le prestazioni vengono valutate attraverso specifici indicatori.

Banda

Capacità teorica della rete.

Throughput

Traffico effettivamente trasportato.

Latenza

Tempo necessario per raggiungere la destinazione.

Jitter

Variazione della latenza.

Packet Loss

Percentuale di pacchetti persi.

9.23 SNMP

SNMP significa:

Simple Network Management Protocol

Permette il monitoraggio centralizzato dei dispositivi.

Informazioni raccolte:

- utilizzo CPU;
- memoria;
- traffico;
- stato delle interfacce.

9.24 Log di Sistema

I dispositivi generano continuamente registrazioni chiamate log.

I log permettono di individuare:

- errori;
- guasti;
- tentativi di accesso;
- problemi di sicurezza.

9.25 Wireshark

Wireshark è uno degli strumenti più utilizzati dagli amministratori di rete.

Permette di catturare e analizzare il traffico.

Funzioni principali

- cattura pacchetti;
- analisi protocolli;
- individuazione anomalie;
- troubleshooting avanzato.

9.26 Analisi dei pacchetti

Attraverso Wireshark è possibile osservare:

- indirizzi IP;

- indirizzi MAC;
- protocolli;
- porte;
- contenuto delle comunicazioni.

Questo consente una diagnosi molto accurata.

9.27 Monitoraggio proattivo

Le organizzazioni moderne adottano sistemi di monitoraggio continuo.

Obiettivi:

- prevenire i problemi;
- individuare anomalie prima che diventino critiche.

Vantaggi

- maggiore disponibilità;
- minori interruzioni;
- migliore esperienza utente.

9.28 Capacity Planning

Consiste nella pianificazione della capacità futura.

Permette di prevedere:

- crescita del traffico;
- incremento utenti;
- necessità di aggiornamento infrastrutturale.

9.29 Caso di studio

Un'azienda segnala lentezza nella navigazione Internet.

Procedura:

1. Verifica fisica dei collegamenti.
2. Test ping verso gateway.
3. Verifica DNS.
4. Analisi traffico con Wireshark.
5. Monitoraggio utilizzo banda.

Risultato:

un server stava saturando la connessione con backup non pianificati.

Dopo la correzione il problema viene risolto.

9.30 Best Practice Operative

Per mantenere una rete efficiente è consigliabile:

- documentare la configurazione;
- monitorare costantemente i dispositivi;
- aggiornare firmware e software;
- verificare periodicamente i backup;
- implementare sistemi di allarme;
- eseguire controlli preventivi.

Riepilogo

In questo capitolo abbiamo studiato:

- progettazione delle reti;
- analisi dei requisiti;
- documentazione;
- troubleshooting;
- modello OSI applicato alla diagnosi;
- ping;
- traceroute;
- ipconfig;
- nslookup;
- netstat;
- SNMP;
- Wireshark;
- monitoraggio proattivo;

- capacity planning.

Queste competenze rappresentano il collegamento tra la teoria delle reti e la gestione operativa quotidiana delle infrastrutture informatiche.

Domande di verifica

1. Quali sono le fasi della progettazione di una rete?
2. Perché è importante la documentazione?
3. Quali passaggi caratterizzano il troubleshooting?
4. Come può essere utilizzato il modello OSI per diagnosticare problemi?
5. A cosa serve il comando ping?
6. Qual è la funzione di traceroute?
7. Cosa mostra ipconfig?
8. Qual è il ruolo di nslookup?
9. A cosa serve SNMP?
10. Perché il monitoraggio proattivo è importante?