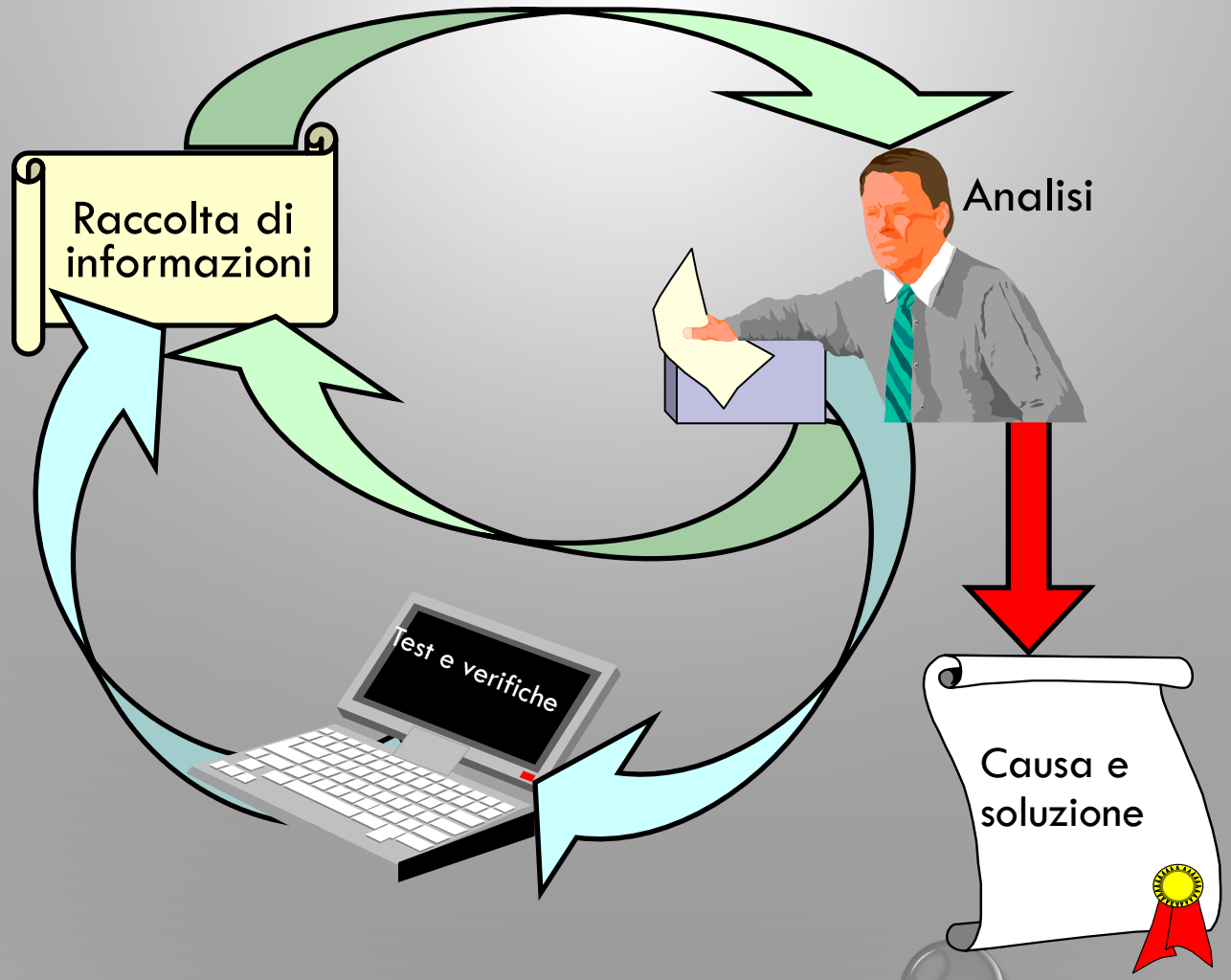
TROUBLESHOOTING E ANALISI DEL TRAFFICO DI RETE

(Pietro Nicoletti)

RICERCA DELLA CAUSA DI UN PROBLEMA

- UN PROBLEMA O UN GUASTO DI RETE VA AFFRONTATO CON METODOLOGIA E TECNICHE INVESTIGATIVE
- BISOGNA, INNANZI TUTTO, AVERE UN'ADEGUATA CONOSCENZA DEGLI ASPETTI TECNICI PER INTERPRETARE CORRETTAMENTE LE INFORMAZIONI INERENTI AL PROBLEMA CHE SI ANALIZZA
- A FRONTE DI UN PROBLEMA SI INIZIA CON LA RACCOLTA DI TUTTE LE INFORMAZIONI POSSIBILI

CICLO DI ANALISI DEL PROBLEMA



CICLO DI ANALISI DEL PROBLEMA

- IL CICLO DI ANALISI SI PUÒ RIASSUMERE FASI:
  - RACCOLTA D'INFORMAZIONI
  - ANALISI DELLE INFORMAZIONI RICEVUTE, CHE PUÒ DAR LUOGO AD UNA SUCCESSIVA RICHIESTA DI DATI
  - TEST E VERIFICHE
    - POSSONO SERVIRE PER FORNIRE ULTERIORI DATI NECESSARI PER L'ANALISI DEL PROBLEMA
    - SONO UTILI PER VERIFICARE LA CAUSA DEL PROBLEMA IPOTIZZATA E L'EVENTUALE SOLUZIONE

INFORMAZIONI UTILI PER L'ANALISI

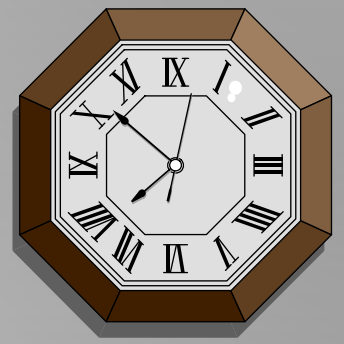
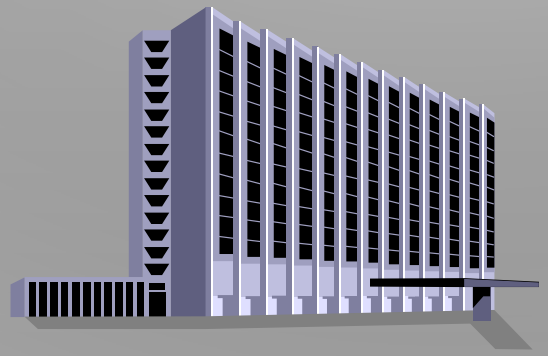
- INFORMAZIONI UTILI CHE AIUTANO A CIRCOSCRIVERE IL PROBLEMA:
  - DATI CHE AIUTANO A STABILIRE IL NORMALE COMPORTAMENTO DELLA RETE
  - QUANDO E CON CHE FREQUENZA SI VERIFICA IL PROBLEMA
  - COME SI MANIFESTA IL PROBLEMA
  - QUALI SONO LE PARTICOLARITÀ LEGATE AL TIPO DI MANIFESTAZIONE O AL MOMENTO IN CUI SI VERIFICA IL PROBLEMA
    - EVENTI NON COMUNI, PICCOLI O GRANDI EVENTI CHE SI SCOSTANO DALLA NORM

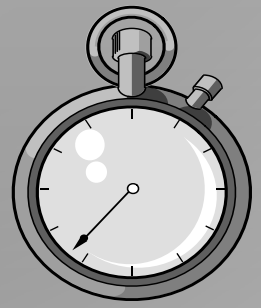
ANALISI

- PER PRIMA COSA BISOGNA STABILIRE LA CONDIZIONE DI *NORMA*
  - A FRONTE DI QUESTO DATO DI POSSONO DEFINIRE GLI *SCOSTAMENTI*, QUINDI I POTENZIALI PROBLEMI
- BISOGNA TENERE UNA TRACCIA SCRITTA DI TUTTE LE FASI DI ANALISI
  - PER POTER EFFETTUARE DEI CONTROLLI A POSTERIORI
  - PER CONFRONTARE DATI ED IPOTESI DI CAUSA
  - ORDINE E MINUZIOSA CATALOGAZIONE DI DATI SONO UNA CHIAVE DI SUCCESSO

COME CIRCOSCRIVERE UN PROBLEMA

- BISOGNA STABILIRE:
  - *QUANDO* SI VERIFICA
  - *DOVE* SI VERIFICA
  - *COME* SI MANIFESTA
  - *IN QUALI CONDIZIONI* SI MANIFESTA
  - *CON QUALE FREQUENZA*
  - ANALIZZARE CON ATTENZIONE EVENTUALI *PARTICOLARITÀ O PICCOLI SCOSTAMENTI* DALLA NORMA CHE SI VERIFICANO CON L'EVENTO



MONITORAGGIO DEL TRAFFICO DI RETE E REPORTING

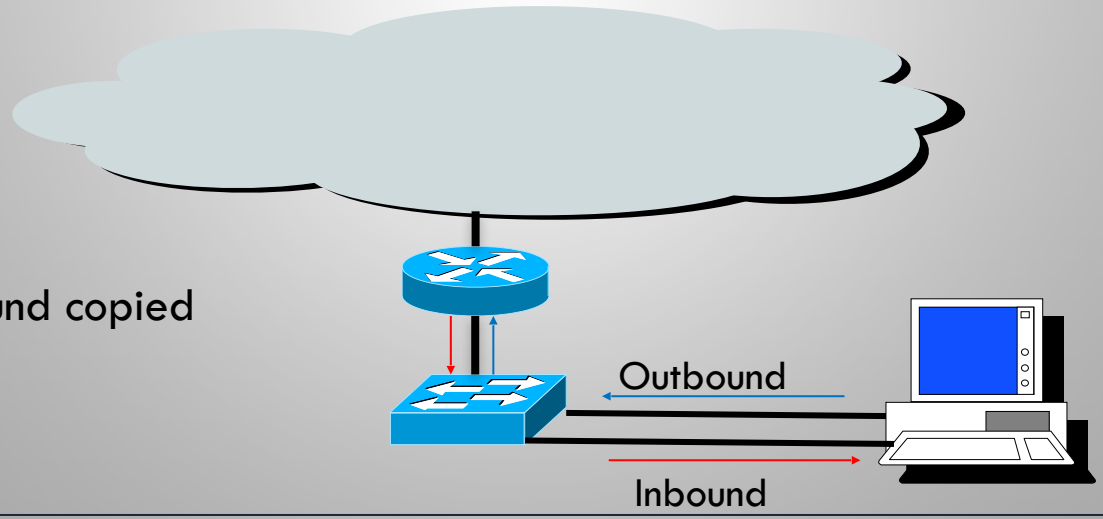
- IL MONITORAGGIO È UTILE PER AVERE UN CONTROLLO COSTANTE E CONTINUO DEL TRAFFICO DI RETE, SPECIE SE ASSOCIATO AD UN REPORTING PERIODICO, ED È INDISPENSABILE PER IL PROBLEM SOLVING
- IL REPORT PERIODICO DEL TRAFFICO DI RETE AIUTA A STABILIRE LE CONDIZIONI DI NORMA
- L'ANALISI PUNTUALE DEL TRAFFICO DI RETE E DELLE CARATTERISTICHE DEI FLUSSI AIUTA A STABILIRE GLI SCOSTAMENTI

COME ANALIZZARE IL TRAFFICO

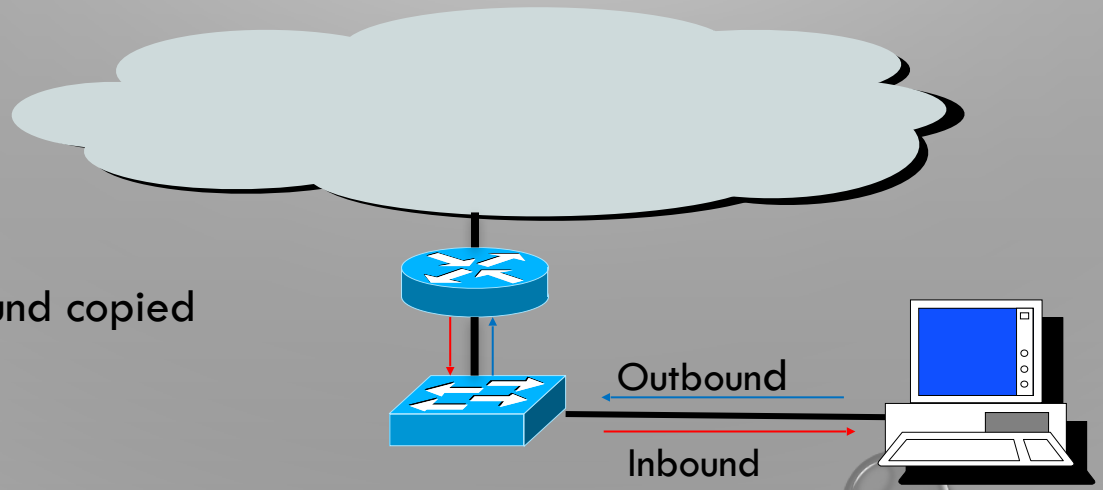
- PER ANALIZZARE E VERIFICARE IL TRAFFICO QUESTO DEVE ARRIVARE ALL'INTERFACCE DI RETE DELLA SONDA O SERVER ADIBITO ALLO SCOPO. LE SOLUZIONI POSSIBILI SONO DUE:
  - COPIARE IL TRAFFICO PROVENIENTE DA UNA PORTA DI UNO SWITCH SU UN'ALTRA PORTA CONNESSA ALLA SONDA O SERVER DI MONITORAGGIO.
    - MIRRORING, TERMINE COMUNE
    - SPAN (SWITCHED PORT ANALYZER), TERMINE CISCO
  - IMPIEGO DI TAP PASSIVI PER LE CONNESSIONI OTTICHE
  - IMPIEGO DI TAP ATTIVI PER LE CONNESSIONI RAME

LA COPIA DEL TRAFFICO: MIRRORING O SPAN

Inbound & Outbound copied on different ports



Inbound & Outbound copied on the same port

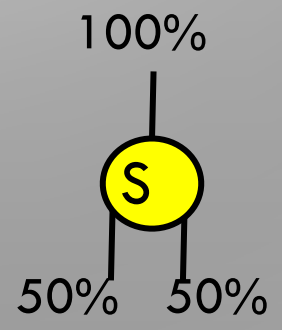


PORT MIRRORING: VANTAGGI E LIMITI

- VANTAGGI:
  - NON RICHIEDE L'IMPIEGO DI TAP CHE VENGONO INSERITI IN MEZZO ALLA CONNESSIONE E DIVENTANO UN SINGOLO PUNTO DI FAILURE.
- SVANTAGGI
  - SE VIENE FATTA LA COPIA DEL TRAFFICO INBOUND E OUTBOUND (DIREZIONE " BOTH" CHE È IL DEFAULT) LA BANDA AGGREGATA È TEORICAMENTE IL DOPPIO DELLA BANDA DELL'INTERFACCIA SU CUI VIENE COPIATO IL TRAFFICO.
    - POSSIBILITÀ DI PERDITA DI PACCHETTI (DROP)
  - ALCUNI SWITCH ECONOMICI AMMETTONO UNA SOLA SESSIONE, ALTRI DUE SESSIONI, I PIÙ EVOLUTI E PERFORMANTI AMMETTONO PIÙ SESSIONI

IMPIEGO DI TAP PASSIVI: VANTAGGI E LIMITI

- SI USANO DUE TAP, UNO PER OGNI DIREZIONE TX E RX
- VANTAGGI:
  - NON CI SONO PERDITE DI PACCHETTI DOVUTI ALLA SATURAZIONE DELLA BANDA
- SVANTAGGI:
  - SEBBENE PASSIVI POSSONO ESSERE DIFETTOSI E POSSONO IMPATTARE SUL TRAFFICO DI RETE E/O INTERROMPERE LA COMUNICAZIONE
  - POSSIBILI PROBLEMI SULLE CONNESSIONI IN FIBRA OTTICA MULTIMODALE A CAUSA DEL SUPERAMENTO DELLA SOGLIA DI ATTENUAZIONE
- I TAP PASSIVI SONO DEGLI SPLITTER OTTICI A DUE VIE
  - POSSONO ESSERE 50/50
  - POSSONO ESSERE 30/70



CASI REALI DI TROUBLESHOOTING E CONTRIBUTO DI NTOP ALLA SOLUZIONE

- TRAFFICO ANOMALO NOTTURNO RILEVATO DA NTOP SU UN PC AZIENDALE
  - NTOP HA RILEVATO L'ECCESSIVO TRAFFICO E CHI L'HA GENERATO
    - IL PROBLEMA ERA CAUSATO DA UN TROJAN
- SATURAZIONE DELLA BANDA INTERNET A SEGUITO DI PROBLEMI DI GESTIONE DEGLI UPDATE
  - NTOP HA RILEVATO I PROTOCOLLI APPLICATIVI E I PC COINVOLTI
- TRAFFICO ANOMALO IN UN ESERCIZIO COMMERCIALE CHE BLOCCAVA IL TRAFFICO INTERNET E INTERAZIENDALE TRA LE SEDI CON CONSEGUENZE ANCHE SUL BANCOMAT
  - VIRUS SU UN SERVER CHE APRIVA CONTINUAMENTE CONNESSIONI VERSO MIGLIAIA DI SITI, NTOP HA RILEVATO L'ENORMITA' DI CONNESSIONI VERSO INDIRIZZI PUBBLICI E CHI LE CAUSAVA
- LENTEZZA SULLE CONNESSIONI VERSO INTERNET
  - NTOP HA DIMOSTRATO CHE LA BANDA ERA SCARSAMENTE UTILIZZATA E MOLTO SOTTO SOGLIA
  - IL PROBLEMA ERA DELL'OPERATORE DI TLC